Investigations – Computer Forensics – Electronic Discovery

www.renusa.com

March, 2011

Tough Economy Increases Incidents of Intellectual Property Theft:

Critical actions for successful outcomes

Kevin Barrows, Managing Partner, Renaissance Associates, Ltd.

Protecting businesses from the threat of a crippling incident of intellectual property theft is difficult given that today "trusted insiders" can walk away with the crown jewels of trade secrets, client lists or other proprietary data with a simple email attachment or copying to an easily-concealable USB drive. These risks are made greater in a pressing economy as employees leverage stolen IP when seeking new jobs, or if a vendor is motivated by the promise of illicit gains by selling IP to interested parties.

While every IP theft creates unique challenges, companies that were more successful in creating favorable outcomes in these matters took two very decisive steps: first they created an *Incident Response Team and Plan* and secondly implemented *Preventative Measures* to minimize the risks associated with IP thefts.

1. **Create the Incident Response Team and Plan**

   The best defense is a great offense. Prepare the enterprise for inevitable IP thefts and other data loss incidents by creating a team of key company representatives who have well-defined roles and responsibilities and act from a coordinated response plan. The team should consist of members from internal company functions and select outside specialists:

   - In-house and outside counsel
   - Special investigative consultants and digital forensics experts
   - IT and IT security, HR, Compliance/Regulatory/Privacy, physical security
   - Executive management, officer-level liaison

This team should work from a response plan that quickly determines the facts and preserves evidence, including:

- Implementing a thorough investigation strategy – who, what, where, why, when and how
- Conducting a full damage/risk assessment and the impact to the company, their clients and other key stakeholders
- Preserving electronic data in a forensically sound manner so that it can be produced as evidence, and corroborated with expert testimony, as needed
- Implementing all aspects of the mitigation plan including pursuing potential civil and/or criminal litigation matters
- Conducting incident post-mortem analysis and response results
- Amending policies, procedures and people management issues to prevent similar incidents and better prepares the company for future events

2. Implement Preventative Measures

- *Conduct thorough background checks on employees, vendors and strategic partners.* Comprehensive background checks are powerful tools in rooting out potential perpetrators and preventing IP theft incidents before they happen. These should be conducted for all internal personnel, external vendors who have access to mission critical data or confidential information. Some of these stakeholders may not seem obvious, but even the mundane vendor (i.e. cleaning agency personnel with access to paper files) can pose a threat. Comprehensive background and due diligence processes need to go beyond simple financial checks or criminal violations databases, to include in-person interviews and surveillance for definitive proof or evidence, as individual matters dictate. A complete background check fulfills an important management mandate - to have the best intelligence when making important decisions on potential employees, vendors or partners.

- *Know where your most valuable data is and who has access to it.* As organizations become more sophisticated they create robust databases to share information across the enterprise to facilitate business processes with both internal and external stakeholders. To better prevent IP thefts, ensure that IT, HR and Privacy Policies and procedures are in effect to grant appropriate access and to limit, monitor and report access to mission critical data. These policies should include:

    - Maintaining effective IT security protocols, rights management procedures and ensuring legacy systems, backdoors, terminated or transferred employee access is kept up to date
    - Creating, monitoring and enforcing policies that limit copying or downloading to home computers, USB or portable devices including cell phones
    - Extending all IT management and security policies to include any external companies, vendors, consultants or other strategic partners with access to sensitive information
    - Providing training to all key personnel to guard against social engineering by hackers or inadvertent data breach through equipment loss or password leaks
    - Installing encryption measures for database repositories, mobile computers and other at-risk electronic resources to avoid a Personal Identifiable Information data breach or IP theft to computer asset loss
    - Conducting rigorous computer asset audits; verifying lost, stolen, destroyed or returned equipment and disk wiping procedures
    - Creating a proactive reporting function to identify possible suspicious data access activity (i.e. financial data just prior to quarterly reporting or download spikes from an employee who has given resignation notice) and is reviewed for possible further investigation

- *Establish absolute physical environment security.* From the placement and image capture capabilities of security cameras, to adhering to document retention policies and proper shredding procedures, to enforcing keycard access to the physical office or plant can make the difference in preventing crimes of opportunity and provide unmitigated evidence during the investigation or litigation phases.

  The exact nature of the business – if it has public reporting requirements, or is in a highly regulated industry – will impact the focus and implementation of these critical steps. However, any organization that puts efforts into these essential preparations will greatly reduce the occurrence of incidents, be better equipped to act decisively, promptly mitigate risk, and, more quickly respond to and recover from the harm caused by the theft of Intellectual Property. ✧

About the Author:

Kevin Barrows is a Managing Partner at Renaissance Associates, Ltd. with over fifteen years of experience investigating and resolving complex, white collar crime matters for government and commercial parties. Mr. Barrows is a licensed attorney in the State of New Jersey, a former, highly decorated FBI special agent and a widely regarded expert in the areas of white collar crime, computer fraud and due diligence investigations. He can be reached at kbarrows@renusa.com, 973-828-6705.

About Renaissance Associates, Ltd.

Renaissance Associates, Ltd. is a specialized advisory firm lead by highly experienced, former Federal Agents from the United States Postal Inspection Service and the Federal Bureau of Investigation. The firm provides comprehensive services to corporations and leading law firms by applying years of field-proven investigative skills and computer forensics expertise in the areas of corporate fraud, intellectual property theft, data breach, cyber crime, financial fraud, due diligence, background investigations, electronic discovery and expert witness services.

For more information go to: http://www.renusa.com.