

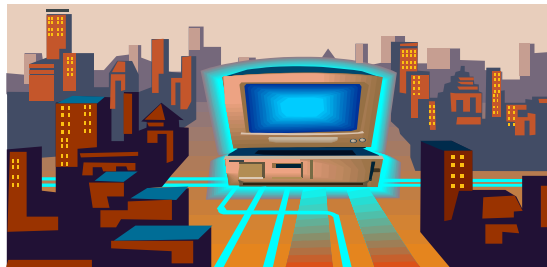
INNOVATIVE CORPORATE SOLUTIONS, INC.



"PIONEERING THE FUTURE FOR INFORMATION SECURITY"

Innovative News

SECURING YOUR INTELLECTUAL PROPERTY



The growing concern with the security around Intellectual Property has emerged as one of the plagues in the 21st century. The new era of business has brought more complex issues as to how companies are protecting their intellectual property. UC Berkley reported in a recent study that around 92% of the company's documentation is stored in a digital format. As companies seek to become more of a paperless society the risk becomes greater for businesses to protect their intellectual property. The major issue in many intellectual property cases is did the company protect the resources that were claimed to have been violated or stolen. The FBI reported in 2003 that Intellectual Property or the theft of proprietary information totaled \$70,195,900, the biggest financial loss for companies based on a small number of businesses that did report. These numbers come from companies that voluntarily report these incidents to the FBI to generate the basis of the security concerns. If all the companies would be forced to report the numbers would be frightening for companies to get a true picture of where the security is in our nation. Security can assist in the efforts to focus on the reduction of the vulnerable concern of Intellectual Property theft.

Securing your
Intellectual
Property:

Where is Intellec-
tual theft is coming
from?

As a company
what can I do to
lower my risk of
exposure of my In-
tellectual Property
theft?

Future of impor-
tance of Intellec-
tual Property theft?

Writing by:
Innovative-CSI
Duane Hopkins,
Security Consultant



**INNOVATIVE
CORPORATE SOLUTIONS, INC.**

"PIONEERING THE FUTURE FOR INFORMATION SECURITY"

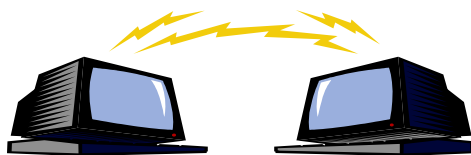
Where is Intellectual theft coming from?

Common occurrences of intellectual property typically comes from the internal workings of your own company environment. Examples of internal threats to your company would consist of the access of an employee, contactor, or guest. The internal threat of the organization is due to the confidential information and access that employees are given during their employment with the organization. The FBI reports in 2004, 59% of the attacks are the internal users of the system. The resolution is the restructuring of the security measures around the organization's access controls and conducting regular audits of the systems and plans. External threats to intellectual property are coming from a variety of different directions. The most common is corporate espionage, hacking and identity theft. Corporate espionage cases are becoming more common as competitor companies are trying to get an edge on being the best in the niche. Competitor companies have gone to the extremes to hire hackers to provide a Denial of Service attack (DoS) of the opposing website along with a number of other activities. The goal in corporate espionage is to steal trade secrets, financial data, confidential client lists, marketing strategies or other information that can be used to sabotage the business or gain a competitive advantage.

As a company what can I do to lower my risk of exposure of Intellectual Property theft?

The company responsibility is to provide the due care in protecting its efforts to protect the resources. Securing the intellectual property of your company is not a one stop answer to resolve the issue. Companies need to look at the level of risk that resides around the core of the business. A customized solution to your security plan should combat and encompass the companies overall security goals in keeping it secure. When looking at securing your Intellectual Property your security plan should include the following at a minimum:

- Business Continuity and Disaster Recovery Plan current and up-to-date
- Current and up-to-date Incident Response Plan
- Examination and Re-examination of the company policies and procedures
- Expert on staff or on call in Computer Forensics
- Audits and penetration testing of the systems
- Solid Security Solutions based off of the risk analysis of the company



***“Working with an
Expert
Consultant in
Computer
Forensics will
result in big ROI
for the company’s
future”***



Having a good working plan in place will help and combat when an incident occurs in your organization. Shifting the company's paradigm from luxury item or I will look at security when I need it, to being prepared with plans and expert consultants when the incident occurs is the future. In security, the phase is not if an incident will occur, it is always when it will occur. The organization should have incorporated in the plan to make the plan more effective in the implementation of an expert in computer forensics. Computer forensics investigation is crucial in the detection of the incident and the only way to prove if your intellectual property has been stolen. The most important piece of the security puzzle is to have an expert to preserve the evidence and to have a plan to stabilize the company's success for the future. Computer forensics investigations help to defend their property and recoup their losses as the company proceeds with legal action. The ROI for companies that are staying on the fore front of security issues are seeing the benefits of having an expert and plans in place. As a consultant in the information security field the biggest vulnerability comes from the small to medium size companies. Large corporations are already complying with federal laws that mandate them to comply with Sarbanes-Oxley and Gramm-Leach-Bliley Acts. The small to medium size companies have the biggest risk exposure. Properly protecting the resources is the key component to the survival and competitiveness of the small to medium size company.

As a small to medium size company if an attack occurs to your organization remember to:

- Respond quickly and without fail.
- Have key response personnel predetermined.
- Get your key personnel involved early (like your computer forensics expert).
- Consider content monitoring of the attack.
- Determine the cost of the attack.

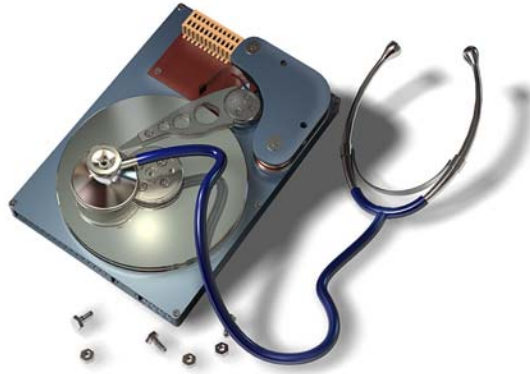
Growing concern of the Importance of Intellectual Property theft?

Professionals in the area of information security and the legal industry see the future problem of Intellectual Property theft is becoming overwhelming worse. As companies prepare to enter the global market in countries like China, Poland and other countries, intellectual property theft will be a greater concern. Securing your company before those transactions take place is the survival and due diligence that needs to occur. Working with good and knowledgeable legal counsel in conjunction with professional security consultants that can assist your business needs in computer forensics investigations along with consulting on security plans and implementation of solid solutions is the focus for companies to succeed. Seeking those professionals insures the reduction and exposure of the risk of intellectual property theft during your business endeavors both here and outside of the country.



How can you protect your company's intellectual property?

Your Security Solution



"We offer one of the most complete & professional investigations by providing a sound methodology to recover your evidence"

Expert Analysis in:

Computer Forensics
Network Forensics

Litigation Support
eDiscovery

Accounting Forensics

Additional Client Service Support in:

Business Continuity
Corporate Investigations
Sarbanes-Oxley Compliance
Corporate Fraud

Incident Response Planning
Network Security
Awareness Training

INNOVATIVE CORPORATE SOLUTIONS, INC.

248.846.8600

www.Innovative-CSI.com