

Computer Forensics

IRG's methodologies and best practices lead the industry. Cases have been lost because a plaintiffs electronic discovery "expert" improperly handled evidence. Once we have preserved the evidence, IRG will work to establish the facts in dispute and answer your questions.

Litigation Support

With advances in technology, now more than ever lawyers must be tech-savvy; now they have to be prepared to jump head first into possibilities of evidence discovery far richer than the paper documents the legal profession has historically relied on. For this reason IRG has developed several offerings designed specifically to aid legal counsel with electronic data issues. Let us help you with the following issues.

Electronic Discovery Issues - Plans, Analysis & Drafting Assistance.

- Fed. F. Civ. P. 16(c) Pretrial Conference Agenda for Computer-Based Discovery
- Fed. F. Civ. P. 30(b)(6) Deposition Notice & Compliance Analysis
- Evidence Preservation Letters (Re: electronic media)
- Preparing discovery requests tailored to individual circumstances - Interrogatories, Requests for Production & Admissions
- Database Record Extraction and Analysis

Expert Testimony

- Forensics on all computer media from local hard drives to the most complex of servers
- Court Appointed (Independent) Expert (with protocols)
- Locating & restoring "missing" or deleted electronic data
- Motions to Compel Electronic Discovery - *Analysis and supporting testimony for "burdensome", "accessibility" & "availability" arguments*

Education

Classes are presently being offered on the following topics:

- Incident Response
- Computer Forensics
- Advanced Topics in Computer Forensics
- Ethical Hacking
- Electronic Discovery - A legal and Technical Perspective

All classes are "hands-on" to provide each student with the maximum opportunity to learn. Corporations desiring in house training for groups of 5 or more may contact IRG directly to request a quote or schedule a class.

Contact

For more information please visit us at <http://www.inforiskgroup.com> or contact us via any of the following methods:

Phone: 954-874-1701
Fax: 954-874-1699
E-mail: inforisk@inforiskgroup.com
Mail: 3350 SW 148th Avenue, Suite 110
Miramar, FL 33027

Offering Information Security and Risk Management services to companies throughout the Americas.

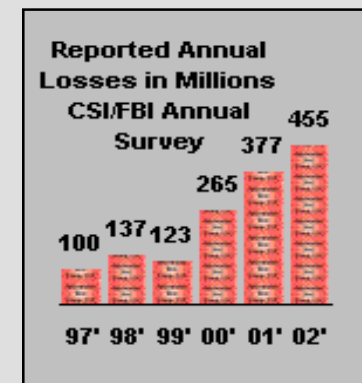
© Copyright 2004 Information Risk Group LLC. All Rights Reserved.



"Offering Information Security and Risk Management services to companies throughout the Americas."

Shawn Acker, CIO

The FBI together with the Computer Security Institute have reported an annual increase in monetary losses from cybercrime for each of the past 6 years. Most recently in the year 2002 survey, losses reached \$455 million. A \$455 million actual loss for the 503 companies that the FBI/CSI surveyed. Estimates are that total losses in the U.S. currently reach US\$ 45 Billion a year.



According to the study the majority of these losses may be categorized into the following areas:

- theft of intellectual property
- financial fraud
- viruses
- insider abuse of the network
- system penetration from the outside
- sabotage of data networks.

Don't become a statistic. Your company can take steps to mitigate the risk posed by these threats. The question you should ask yourself is not if this is going to happen to your company, but when will it happen to your company. Just as you physically lock the doors of your company and secure your money in a bank; you must logically secure your computers and networks.

Our staff has worked for some of the largest companies in the Fortune 500. Let the experts at IRG help you assess and mitigate your risk.

How IRG can help you

For information technology to bring your company a high return on investment it must not only enhance your corporation's productivity it must protect your corporation's digital assets. IRG has developed an enterprise wide information security strategy ready to address your security concerns.

Security Assessments

Information security assessments benefit companies by focusing management on areas where reputation and strategic risk can be reduced. Understanding risk requires the analysis of a wide range of information relevant to a particular company's risk environment. IRG's holistic assessment methodologies are based on the years of experience our employees have working with large financial institutions and major accounting firms. An annual security assessment should be considered an essential metric of every companies ongoing security strategy.

Information Risk Group LLC has developed several services to meet the changing needs of our customers:

- Customized Security program development/Risk Analysis
- GLBA Safeguard Assessments
- HIPAA Safeguard and Privacy Assessments
- Firewall, IDS and DMZ Assessments
- Information Security Policy and Standard Gap Analysis

All reviews are performed in an efficient and timely manner in order to minimize any impact to your company and its personnel. As independent examiners of your company's overall security strategy, IRG is in a position to offer impartial reporting on the effectiveness of a company's information security implementation. Contact IRG today to discuss which security assessment solution is appropriate for your company.

Ethical Hacking

An ethical or "white hat" hacker is an excellent way to test your systems vulnerabilities from the outside. Information Risk Group proprietary Attack and Penetration Methodology (APM) is designed to provide maximum results with minimum system impact. Working closely with your staff, our security team attempts controlled penetrations of your networks and other points of access. Controlled penetrations are designed to do no harm to your systems. This ensures maximum uptime for your systems and prevents outages that may affect your company's customers.

In the event a serious misconfiguration or vulnerability is discovered it will be immediately reported to the customer for remediation. All findings are independently verified using a second distinct methodology; this effort prevents "false positive" reporting. IRG also rates each finding into two categories: ease of repair and difficulty to perform exploit. This allows you to concentrate on which problems you can fix given your resources.

Incident Response

Information Risk Group is prepared to implement the latest tools and techniques to verify, suspend and trace an incident against your systems. We will help you mitigate the affects of an attack against your systems.

Our emergency response team has worked with the FBI, the US Customs Service, and state authorities on various cases throughout the years and is available to offer our expertise in this area 24 hours a day.

Emergency Response

Active incidents require experience and advanced knowledge to solve. Time is of the essence. Let us help you mitigate your losses by providing the necessary expert services to resolve your crisis. If you are presently facing a computer incident that you believe may be related to a computer crime contact IRG now for a consultation.

Technical Investigations

Has your company face any of the following situations:

- Intellectual Property Theft
- Email or Internet Abuse
- Internal Hacking Attempts
- Sexual Harassment Charges
- Corporate Ethics or Policy violations
- Sabotage to electronic systems

IRG is prepared to handle these situations in a discreet and confidential manner to protect your company's reputation, build a case for disciplinary actions or establish evidence required to report a criminal action to the authorities. We follow strict guidelines with respect to evidence handling as set out by the United States Federal Government's Department of Justice. In addition to conducting a technical review of the systems under investigation, if desired we will also conduct interviews with all individuals involved in the situation to further clarify our results.