

KLINK & CO., INC.

A Global Leader in Risk Consulting

Communiqué

COMPUTER FORENSICS – A NEW TOOL IN LIMITING LIABILITY

The following is a Klink & Co., Inc. Communiqué discussing issues facing attorneys and corporate counsel.

While computers can increase your company's productivity and profitability, they can also be the source of liability. However, your exposure can be limited by using tested and cost effective computer forensic techniques. These techniques can aid you in identifying and eliminating liabilities before they arise and assist in preparing for litigation.

“We're under attack.”

CASE STUDY

A corporation in a business disparagement case retained Klink & Co. The client sought to determine who was distributing false information about it to its clients and to the public. The client had copies of the disparaging letters but had no leads on the source.

A computer forensic investigation uncovered not only the identity of the author (an employee), but also, that the employee was violating corporate computer policies by accessing “subject inappropriate” websites. The employee was confronted and resigned immediately.

Corporations and their computer systems are often “under attack” from external and internal sources. The assaults may be from outside “professional” hackers, disgruntled employees or individuals who post inappropriate or confidential information on Internet message boards.

The key is establishing a defense that thwarts and responds to the attacks while enabling you to conduct business in a normal manner.

Hacking

Hackers present a formidable problem for any organization regardless of size. Working with “inside” IT professionals, we can assist in developing defenses and conducting investigations.

We have found that there are often difficult decisions to consider such as whether to make the intrusion public knowledge by initiating a legal action, civil or criminal.

Disparagement Cases

When the assault consists of disparaging comments and false or misleading Internet postings, tracking the source of the messages is critical. Through the use of high tech and traditional investigative techniques, the identification of the source can be made but requires skill and knowledge.

Working with counsel, we have found that traces can be established and appropriate legal actions taken to end the disparaging behavior.

Inappropriate Use

The accessing of “subject inappropriate” websites, graphic materials and receipt of inappropriate e-mail messages can place a business at risk for – sexual harassment, criminal actions, contract litigation, etc.

Using a variety of tools and methodologies, we assist clients in:

- Determining the presence of inappropriate materials;
- Identifying responsible parties;
- Assessing damage and exposure; and
- Developing a response program.

To combat and identify breaches, we recommend that companies have a clear and precise policy on the use of company computers and that audits take place on a periodic basis. These audits ensure that company computers do not house inappropriate data.

“Where is that order?”

CASE STUDY

A client had two employees resign and join a competitor. Both long-time employees had a vast knowledge of customer lists, sales and other proprietary information. Our client was suspicious of inappropriate behavior prior to the resignations and suspected the former employees were working for the competitor prior to resigning. Indeed, several key projects never arrived despite previous assurances from the customers.

Our investigation included a forensic examination of the computers used by the former employees. The examination of the hard drives revealed that the employees were in fact

actively marketing customers and directly competing for business opportunities while in the employ of our client.

The information discovered in the investigation was successfully used in an action to restrain the employees and competitor from using the proprietary information and competing with the client.

When conducting a forensic computer examination, the key to a successful investigation is discovering the evidence and preserving the evidence for use at trial. Our methodology allows us to extract the data from computer hard drives without altering the evidence. We are then able to thoroughly examine the data in a variety of media while preserving its integrity.

Recovering Deleted Data

Simply because a file or document has been deleted does not mean that it is no longer accessible. Computer forensic techniques enable one to identify, recapture and secure documents that have been deleted.

Encrypted/Password Protected Data

Passwords and encryption can create a variety of problems. They are forgotten or employed as a means to protect data from detection.

Our experts use programs that defeat such protection schemes and enable an organization to gain access to the protected data.

“There’s something missing from these responses.”

CASE STUDY

A client was the subject of a civil action seeking damages for breach of contract. Discovery responses had been directed to the opposing party and sought computer data and files.

Upon receiving the “inadequate” responses, a court order granted an inspection of computers of the opposing party. An extensive computer forensic investigation of the computers was conducted and uncovered:

- *“Damaging” documents that had been omitted from the responses;*
- *Files that had been deleted in an attempt to hide their existence; and*
- *Active participation of the opposing party’s officers in the “cover-up.”*

Our client received a favorable settlement following the investigation.

Computer discovery requests are commonplace in legal actions since significant amounts of data are now stored on computers.

But, the discovery issue cuts two ways. One must seek all computer data from the opposing party and consider if your client is providing all of the information to the opposing party.

Computer forensic services can assist counsel in the discovery support by:

- Assessing discovery requests;
- Identifying and preserving data;
- Retrieving data and extracting relevant information; and
- Producing the data while preserving its integrity for use at trial.

CONCLUSION

Computer forensics is a useful tool for corporate and trial counsel to employ in protecting a company from external and internal attacks, and to uncover and identify facts and witnesses in litigation. This tool enables counsel to become more effective and efficient in representing the company.

The Klink & Co., Inc. Communiqué is prepared in summary form and is not to be construed as legal advice or opinion on any specific fact or circumstance.

For more information regarding Computer Forensics or other services, please call:

Jeffrey Klink, President, 1(800) or email jklink@klink-co.com

Bill Penrod, Vice President, Counsel, (216) 589-9750 and (412) 201-9123 or email wpenrod@klink-co.com

Dave Nolan, Vice President, New York, (212) 292-5116 or email dnolan@klink-co.com