

For Immediate Release
July 31, 2007

For More Information Contact:
Greg Fordham
K&F Consulting, Inc.
Phone: 770-642-0311
Toll Free: 800-335-1188
Fax: 770-642-9913
Email: greg@knfcon.com

**Using Internal IT Staff to Investigate Computer Incidents
Invites the Possibility of Poor Management Decisions Based
on Results Obtained Says K&F Consulting's Greg Fordham**

ALPHARETTA, Ga.—July 31, 2007 – The normal corporate response to a network intrusion, data theft or destruction, or even something as commonplace as an employee misconduct complaint is often to dispatch the internal IT staff to investigate and deliver enough information to senior management that they can evaluate the scope and veracity of the event and take action if necessary.

However K&F Consulting's founding principal, Greg Fordham, thinks that approach is analogous to returning to your home, finding a window broken and your belongings disheveled, and deciding to call the repairman first instead of the police.

Fordham and the members of his firm regularly advise clients on how to respond to computer based incidents.

According to Fordham there are some very basic dilemmas associated with calling on the internal IT staff members rather than a forensic expert to investigate an incident.

"The IT mission is to operate and maintain an organization's computer systems. They are usually not well suited for incident response since they are not trained to collect and preserve digital evidence," Fordham said.

Using the same skills that they would use to install a print driver, Fordham said IT staffers will likely, at a minimum, change important date and time stamps, lose volatile memory, and change or overwrite free space.

"Even if the consequence of these blunders can be neutralized, they still bring

(more)

Add 1 -- Using Internal IT Staff to Investigate Computer Incidents

complexity and cost to any subsequent litigation that may be initiated. And their actions could also raise doubt about the authenticity of significant evidence,” Fordham said.

Fordham also said the lack of forensic analysis training and experience could result in telltale signs of wrongdoing going unnoticed.

“The average IT staff member may not be aware of the additional data resident in many computer system artifacts or even how to interpret them. Without the knowledge of their existence or how they could be used, false conclusions could be reached,” he said.

A discussion paper written by Fordham, *Incident Response: The First Step in e-Discovery*, may be downloaded without charge at www.knfcon.com/IRFirstStep.pdf

Fordham has written extensively on forensic auditing and e-discovery matters. He is a contributing writer for the *2007 Construction Law Update* which was published earlier this year by Aspen Publishers and the Georgia Bar Association has approved his e-discovery presentation for CLE credit.

About K&F Consulting

With offices located in the metro Atlanta area, K&F Consulting services a nationwide clientele. The firm provides a variety of e-discovery and computer forensic services including database forensics, software forensics as well as the more well known forms of computer forensics.

For more information visit the company’s web site, www.knfcon.com.