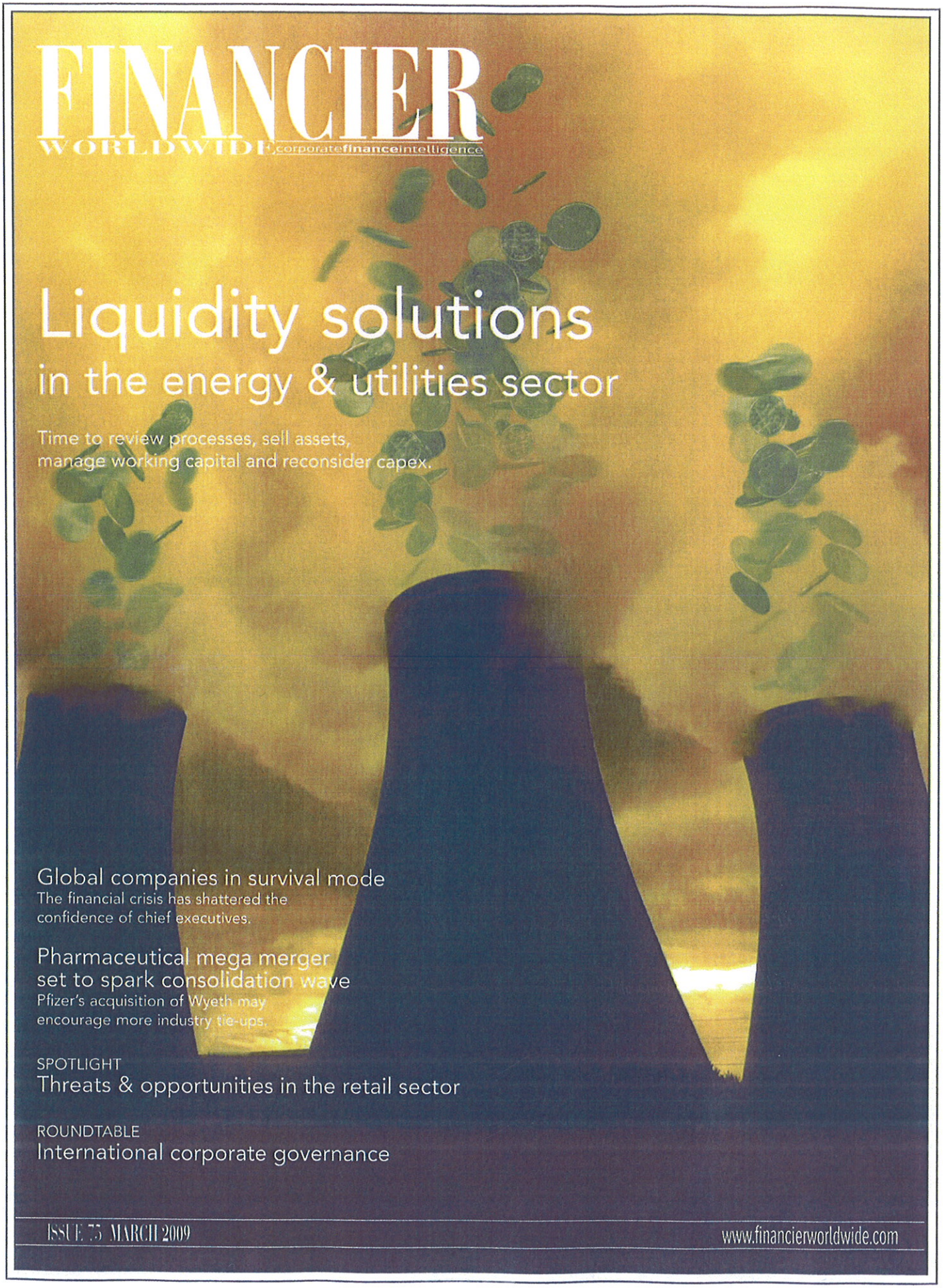
FINANCIER
WORLDWIDE corporatefinanceintelligence



Liquidity solutions
in the energy & utilities sector

Time to review processes, sell assets, manage working capital and reconsider capex.

Global companies in survival mode
The financial crisis has shattered the confidence of chief executives.

Pharmaceutical mega merger set to spark consolidation wave
Pfizer's acquisition of Wyeth may encourage more industry tie-ups.

SPOTLIGHT
Threats & opportunities in the retail sector

ROUNDTABLE
International corporate governance

ISSUE 75 MARCH 2009 www.financierworldwide.com

The 'science' of open sesame – unlocking secrets in a digital world

It's Friday morning. At the other end of the phone, the company's President hears the words, "We have a problem". Fraud allegations have surfaced involving a current employee. Timing is critical. Accurate facts can be difficult to determine. Uncoordinated responses by dispersed employees can incur devastating consequences. The next steps taken by the company are critical to the success or failure of the investigation.

Unfortunately, there are so many ways organisations can fall victim to fraud, but there's really only one way to handle it: get control of the situation ASAP. Proper, timely, coordinated response will limit the financial and reputational damage to the organisation.

It is widely believed that over 90 percent of today's information is created electronically – and much of that never makes it to paper. As such, most organisations rely heavily on technology to conduct day-to-day business – that invariably results in computers and other electronic devices becoming used to perpetrate white collar crime.

Companies may fail to realise they have fallen victim to fraud until their intellectual property (IP) is displayed in the hands of a competitor. An employer may become aware several months (or even years) after the departure of a former, senior employee that the individual joined a competitor – in and of itself, not unusual. The passage of time and the recirculation of the former employee's computer decreases the likelihood of finding potentially relevant evidence that will be admissible, to confirm or dispel suspicions of IP theft. The circumstances could have been entirely different, had the former senior employee's hard drive been forensically imaged and preserved upon their departure.

Take for instance the large corporation that discovers a grey market product is being sold under its name. Forensic analysis of several computers performed at the company reveals that external devices were connected to one of the product development team's computers and that there was unauthorised access to files, which were copied to another device. Forensic analysis performed of the 'destination' device, (i.e., to which the files were copied) confirms the existence of blue prints and digital photos, which were removed without authorisation. The investigation reveals that an estimated $1m in IP had been misappropriated. However, all target sources to which the IP was copied were identified and the files had not been distributed to any other parties.

Investigating fraud allegations

In the unfortunate circumstance when an organisation suspects it has fallen victim to fraud or malfeasance, the company must take steps expeditiously to assess the situation and contain the problem – in order to prevent further losses. Given technology is a predominant source of information, it is important to identify and secure all possible sources of evidence, particularly electronic data that may be relevant to the investigation, including all corporate assigned computers, BlackBerrys, PDAs, mobile phones, USB drives, digital cameras, memory cards and external media. Any user activity on such devices should be discontinued to prevent such evidence from being spoiled.

While company IT departments can assist to identify electronic data-storing devices assigned to particular employee(s), any activity on such devices can alter or destroy the evidence and possibly impede its admissibility. Therefore, the forensic acquisition of such devices should be performed by computer forensics professionals.

All evidence – electronic or otherwise – collected during the course of an investigation must be carefully documented to maintain chain of custody over such evidence, including the date and source from which the evidence was obtained.

Before any analysis can be performed, a bit-stream image (identical copy) of the hard drive or the electronic device containing all resident data must be performed, which will include deleted data. It is important to create backup copies for all electronic evidence seized and original evidence must be stored in a secure environment. Analysis should never be performed on original evidence.

An investigation is required to answer the questions: How was the alleged fraud committed? Who was involved? What was taken and where is it now? What is the financial impact, if any on the company?

Utilising specialised proprietary forensic hardware and software, computer forensics examiners can perform analysis of electronic devices, in order to: (i) extract, reconstruct and recover deleted files, user-created files, password protected files, electronic mail (corporate and web-based) and internet history; (ii) establish what devices have been attached to the user's computer, which is particularly useful when investigating theft of IP allegations; (iii) determine what files have been accessed, printed or modified; and (iv) review for modification of electronic files by correlating to hard copy business records.

Such bits and pieces of data can reveal important information not otherwise available to the company's IT department. Additional evidence collected during the investigation, such as hard copy business records, background intelligence and information obtained through oral interviews will collectively play an important role in gathering the facts.

Once the investigation is complete, a written report may be required to support the Company's fidelity claim, which is an insurance policy against employee malfeasance. Fidelity policies may include an allowance for costs incurred to investigate the alleged fraud. If the Company suffers monetary damages from the alleged fraud, the report can also be used in support of a civil litigation against the involved person(s) to recover damages suffered. Similarly, the company may wish to pursue criminal action by involving law enforcement.

Anti-fraud programs and controls

Prevention – not detection – is the best fraud deterrence. In an attempt to stay 'ahead' of the white collar criminals, companies should have robust anti-fraud program and controls that would include a code of conduct / anti-fraud policy, periodic fraud risk assessment, strong and visible corporate and IT governance and an ethics hotline to report alleged malfeasance.

However, it goes beyond simply documenting policies and procedures and filing them in a drawer. Many companies that have been victimised by fraud invest significant resources to document their policies, but fail ▸▸

to recognise one of the most basic fraud prevention/detection controls – its own employees. Periodic fraud training provides employees with the knowledge and tools necessary to spot questionable transactions and how to report them to the appropriate level within the organisation. According to a 2008 Fraud Survey, tips were the most common means of fraud detection based on the companies surveyed, with 46 percent of cases being detected by tips, up from 34.2 percent in 2006, according to the ACFE 2008 Report to the Nation on Occupational Fraud & Abuse.

While some organisations have IT policies to guide employees regarding appropriate use of corporate IT assets (including internet usage), password requirements, etc., such policies are seldom monitored for compliance. As such, companies may not consider the potential risks or damage – reputational or otherwise – associated with employee internet activity, such as online gambling, downloading and distribution of copyrighted material or exposure to viruses.

In summary, when an organisation is faced with a fraud allegation, it must be organised, maintain discretion and focus on evidence identification and preservation. There may be a tendency to jump to conclusions and / or make premature decisions regarding an individual's employment status without adequate investigation. However, a carefully planned and properly executed investigation that involves consultation with legal and forensic professionals, will always prevail and mitigate further potential damage to the organisation. ■

Edward Nagel is a Principal with Giffin Koerth Forensic Engineering and Accounting and heads up the firm's Forensic Accounting Group. John Young is an Associate at Giffin Koerth, responsible for the firm's Computer Forensics Group. They can be contacted on +1 (416) 368 1700 or by email: enagel@giffinkoerth.com