

**Men don't have monopoly on corruption**

OPINION PG30



**Pursuing money-making opportunities**

PERSONAL WEALTH PULLOUT



**Companies should prepare for crises**

OPTIONS PULLOUT

# THE EDGE<sup>TM</sup>

## SINGAPORE

MICA (P) No. 018/08/2006 PPS 1519/9/2007

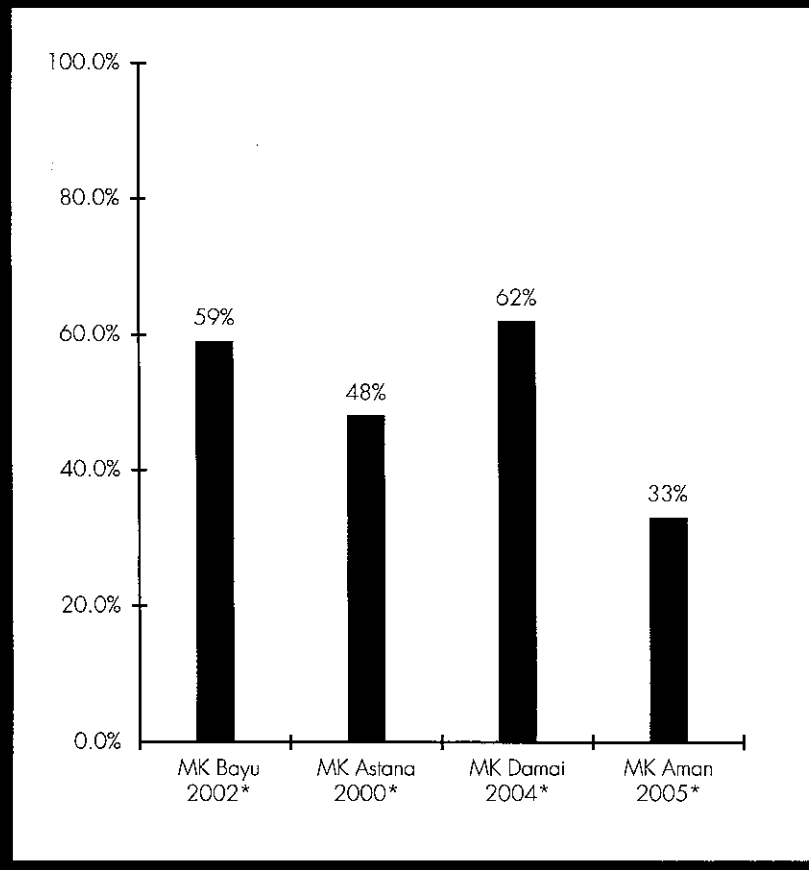
BUSINESS & INVESTMENT WEEKLY

THE WEEK OF OCTOBER 16 — OCTOBER 22, 2006 **238**

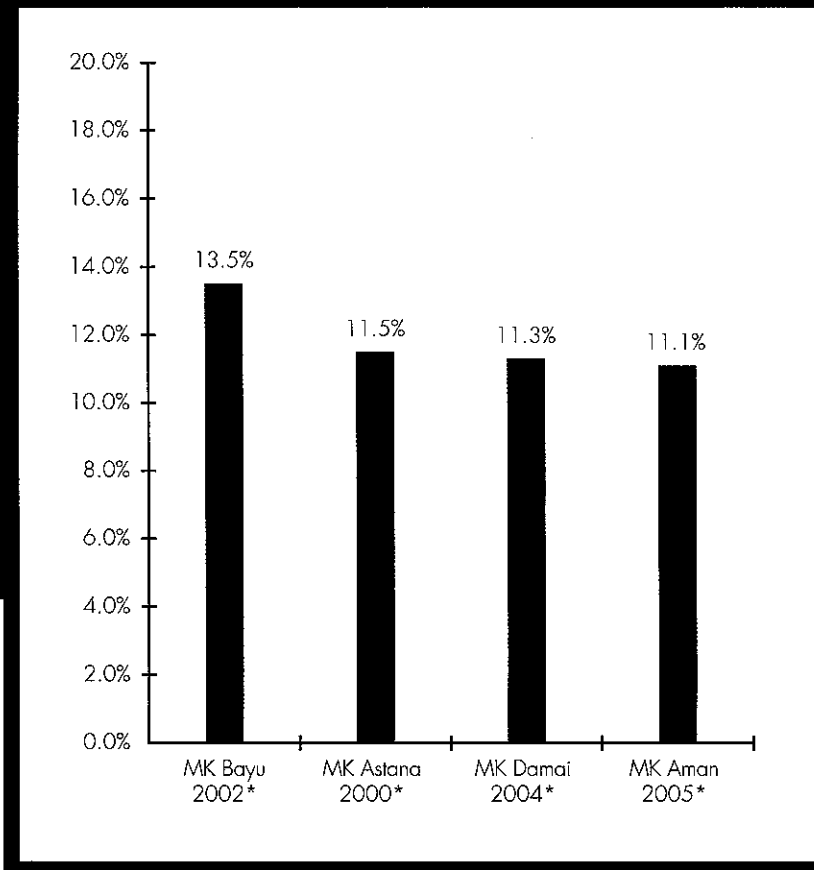
Wise Property Investments = Great Financial Returns

# The Numbers Don't Lie

Capital Appreciation



Rental Yield



*The figures shown here are actual average realised data for the period January - September 2006 of each property from the original launch price to their current market values, and do not include costs of internal renovation or furnishings.*

When it comes to choosing the right Malaysian property developer who can deliver good capital appreciation and rental yields for your investment, you know...

# HP investigators plead not guilty

Former chairwoman and company lawyer to appear in court in November and December

BY JOEL ROSENBLATT

Three Hewlett-Packard Co investigators pleaded not guilty to conspiracy and fraud charges related to the computer company's internal investigation of boardroom leaks.

Ron DeLia, 56, Bryan Wagner, 29, and Matthew Depante, 27, entered pleas before Santa Clara County Superior Court Judge Jerome Nadler last Tuesday in San Jose, California. They were released without bail. Former HP chairwoman Patricia Dunn and company lawyer Kevin Hunsaker, who were also charged in the case, will appear in court at a similar hearing in November and December, respectively, and may enter pleas then.

California Attorney General Bill Lockyer charged the three investigators, Dunn and Hunsaker early this month. He accused them of pretexting, a technique of using fake identities to obtain private phone call records. The records were used to monitor board members and journalists to find the

source of press leaks about the company.

Bryan Wagner "didn't know he was working for HP" when he did the pretexting because he was contracted by Depante's firm to do the research, Wagner's lawyer Stephen Naratil said after the hearing.

California "has a pretty specific law on the books that prohibits" pretexting, Naratil said, adding that Wagner was "never in California" when he did the investigation. Palo Alto-based HP, the world's second-largest PC maker, is also being investigated by the Justice Department and the US Securities and Exchange Commission.

Wagner is a private investigator from Littleton, Colorado. DeLia, of East Sandwich, Massachusetts, heads Boston-based Security Outsourcing Solutions Inc. Depante is an investigator from West Melbourne, Florida. The three investigators are scheduled to return to court in San Jose on Nov 17 for a preliminary hearing at which a trial date will be set.

Depante's lawyer Richard Preira

Former HP chairwoman Dunn and four others face felony charges of conspiracy, wire fraud, illegal use of computer data and identity theft



said his client is innocent and declined to comment further. DeLia and his lawyer John Williams declined to comment.

All five defendants face felony charges of conspiracy, wire fraud,

illegal use of computer data and identity theft. If convicted, they could be sentenced to up to 12 years in prison. The maximum fine for conspiracy to commit identity theft is US\$25,000 (\$1 approx

US\$0.63). The other counts carry maximum fines of US\$10,000. Shares of HP fell seven US cents to US\$37.93 in New York Stock Exchange composite trading. — Bloomberg LP

## Promising future for business intelligence industry

FROM PAGE 20

in Singapore, the tricky part of collecting the information is doing so without tipping off the user of the computer. Typically, the client grants the investigator access to the office after hours to extract information from the computer's hard drive — or, sometimes, the entire hard drive itself. "I took care to leave the office environment undisturbed, which can be harder than it sounds when you are disassembling a computer that is the centrepiece of a desktop with Post-It notes and family photos attached," the computer forensics analyst says.

In one recent case, a private bank hired a corporate intelligence agency that also does computer forensics work to collect information from the computers of several employees who had left the bank. The private bank wanted to know if its former employees had transmitted sensitive client information to external computers before they left. "There is nothing illegal about it because the company who hired us owns the computers," says the corporate investigator.

Besides that, corporate investigators also gather information from sources such as former employees, competitors and suppliers. Anyone who has ever had an encounter with the subject being investigated is a potential source of usual and relevant information. The details that are included in the investigators' reports to their clients could range from the number of times a month the subject visits casinos in Macau to something as subtle as whether he prefers to read *The Straits Times* or the *International Herald Tribune*.

Over time, the business intelligence firms accumulate substantial amounts of data on high-risk individuals and politically exposed people, which they are then able to sell to banks and corporations. One such outfit is World-Check,



As more and more information is aggregated and made available over the Internet, it is becoming increasingly difficult for individuals sporting bogus credentials to keep up their lies — especially when corporate investigators are hot on their trail

which was set up six years ago by its CEO David Leppan to service Swiss bankers who were constantly being accused of harbouring dirty money. "It requires an enormous amount of patience and skill to get out the risk-relevant information from this huge unstructured information that is out there," says Jay Jhaveri, the company's director for Asia.

Jhaveri says World-Check gets its raw information from media reports and sanction lists released by government agencies, such as the US Treasury. It then researches the names and builds a profile of these people through information gathered from several sources — largely Internet websites, but excluding blogs. World-Check adds thousands of names to its list of big-ticket offenders every month. And, the company's clients — which include casinos, yacht brokers, real estate agents as well as banks and government agencies — regularly

cross-check their client lists with the World-Check list.

As more and more information is aggregated and made available over the Internet, it is becoming increasingly difficult for individuals sporting bogus credentials to keep up their lies — especially when corporate investigators are hot on their trail. For instance, degrees from dubious universities sold over the Internet are now being quickly added to blacklists. Supposed institutions of higher learning with reassuring names like American Capital University, Hampton College or Kensington University may not immediately raise many brows. But they are

just three names on a blacklist of 330 questionable universities maintained by the US state of Oregon — one place where you can quickly find names of unaccredited colleges.

A business intelligence professional tells *The Edge Singapore* that in one case, the technical ability of the CEO of a marine company was called into question after he made a series of decisions that resulted in significant losses. The investigators found that people he knew had each been given a different story about his educational path. That made the investigators curious about his degrees, and they eventually discovered that the university from which he was supposed to have obtained a doctorate didn't exist.

### Intelligence versus evidence

Of course, corporate investigators don't always find dirt. In one case, corporate inves-

tigators were called in by a private bank that had become worried that one of its clients was accumulating his wealth through unsavoury activities. The investigators went to the extent of posing as customers and visiting the spas, massage parlours and health clubs he owned that were suspected of being front businesses for prostitution, but they eventually turned up nothing.

Even when incriminating information is found, however, the clients of corporate investigators don't always back away from their dealings with the subject of the investigation. One business intelligence investigator who was hired by a private bank to find out the source of a client's money says the information he obtained pointed to drug trafficking. But it wasn't his job to advise the private bank on what to do. "That is none of our business," he says. "Intelligence is not evidence, after all."

According to most investigators, one out of every 20 reports is negative, and only half of those are potential deal killers. In the end, it comes down to whether their clients feel that the risk of continuing to deal with a particular individual or company is worth it. When large sums of money are involved, they are often prepared to take large risks. "They are quite happy to deal with anyone unless you find out that he is an outright terrorist," says the corporate investigator. Industry people estimate that some US\$1.5 trillion of dirty money from organised crime is laundered every year around the globe. Only a small portion of it is caught, while the rest of it is successfully cleaned and passed along into the banking system.

Little wonder, then, that just about every business intelligence player who spoke to *The Edge Singapore* for this story is confident about the industry's future.

# Are you being watched?

BY GAURI BHATIA

Rooting out money launderers. Uncovering the real source of a private banking client's wealth. Finding out whether employees are defrauding their companies. Even checking whether senior executives have lied about their academic background and professional achievements. These are some of the things that corporate investigators do. As Singapore opens its doors ever wider to international trade, capital flows and foreign executive talent, the business of business intelligence is booming.

Not that you would notice. The industry and its players — by their very nature — maintain a low public profile. They occupy nondescript offices scattered around the CBD, where they rarely entertain visitors. They are vague about whom they deal with, and precisely what they do for them. Some decline to give you even a business card, giving the excuse that they have run out of them or that the cards are in print. And, when you are offered a business card, it might only have a Post Office Box address on it, or the address of a head office located in another country. "We don't want walk-ins," is the excuse given by one of them. "We want to expect people."

On the other hand, they are eager to dispel the notion that they are involved in anything sinister. They strive to blend into the local business milieu, donning inconspicuous corporate attire and calling themselves consultants. They describe their work variously as due diligence, corporate research and — a personal favourite — off-balance sheet risk assessment. "Let me make one thing clear, we are not spies," says one senior employee at a corporate investigations company, as he sat down for a chat with *The Edge Singapore* at a roadside café. In fact, they eschew using the term "intelligence" in relation to their work altogether because of the connotations, even though many of them once worked in the intelligence field on behalf of law enforcement and government agencies.

Indeed, many of them might still be foiling terrorist plots and trailing international drug dealers if it weren't for the burgeoning business intelligence industry, which they estimate is pulling in annual revenues of US\$10 billion (\$1 approx US\$0.63) globally. Checking up on the personal probity of corporate executives at a public-listed company or of high net worth clients of a financial institution might be relatively dull. But in the wake of 9/11 and mega corporate busts like Enron, big businesses around the world are paying up big time for the inside dirt on everyone they deal with, making it highly lucrative work. "We provide accurate and timely intelligence to help clients make business decisions," says David Holloway, chief operations officer of corporate investigation firm International Risk Ltd. "We open eyes."

Besides complying with tougher rules laid down by central banks and financial market regulators, big companies and financial institutions are also spending big bucks on corporate intelligence these days to ensure that their reputations aren't damaged by their clients and counterparties. "Nobody wants to be the bank of [Osama] bin Laden," says Scott Graham, managing director of IntegraScreen.

In Asia, the massive accumulation of wealth, greater cross-border capital flows, and a concerted push by private banks to grow their business are creating lots of work for corporate intelligence professionals. Even longstanding clients of private banks face

As banks worry about the probity of their high net worth clients and the market puts a premium on the personal integrity of corporate bosses, the business intelligence industry is flourishing



Checking up on the personal probity of corporate executives at a public-listed company or the high net worth clients of a financial institution might be relatively dull. But in the wake of 9/11 and mega corporate busts like Enron, big businesses around the world are paying up big time for the inside dirt on everyone they deal with, making it highly lucrative work.

probity checks from time to time. According to people familiar with the practice, banks choose which of their thousands of clients should be subjected to these retrospective screenings by considering a range of risk factors. Wealthy individuals with links to Russia, South America and Indonesia tend to attract more scrutiny, they say. The nature of the business they are in is considered too. For instance, people linked to small companies with unusually large sales revenues are sometimes suspected of money-laundering activity, and it is a matter of time before someone begins probing for information on behalf of their bankers.

Another growth area for the business intelligence industry in Asia is pre-employment screening. A lot of this business is coming from the business processing outsourcing sector in India. Executives at call centres in that country handle a lot of sensitive client information, making their personal integrity a matter of utmost importance to their employers. "We used to do 12,000 pre-employment screenings every month, and the majority was in India," says a corporate investigator, who sold this profitable

business 18 months ago.

In Singapore, off-balance sheet due diligence is now mandatory for companies planning to list. That's helping to fuel the growth of corporate intelligence firms. In these cases, investigators examine the non-financial aspects of the company, enquiring about the personal reputations and experience of the individuals linked to it. Of course, the matter is handled in a low-key and discreet manner. Individuals whom the investigators seek information from are gently asked questions about several different people and companies unconnected with the case, masking what they are really after.

Interestingly, in an era where the market is putting a premium on the personal integrity of senior executives, some CEOs are even hiring corporate investigators to dig up dirt about themselves — just to see what turns up. "American corporate biggies with big egos ask us to find what they fear others can find out about them," says one corporate investigator, who has taken on several such assignments. "And, when we come up with nothing negative or scandalous, they gloat about it." It's the sign of the times.

## Public-domain information

Despite the images that immediately spring to mind, the methods used by corporate investigators are hardly the stuff of television shows and spy thriller novels. They don't hack into your e-mail account, tap your phone line or comb through the contents of your rubbish bin for evidence of impropriety. And they don't pretend to be someone they are not in their pursuit of information about people or companies. For the most part, the information they acquire comes from the public domain — it's amazing what you can find on the Internet. "Eighty per cent of what we include in an intelligence report is publicly available," says Simon Goddard, managing director of Global Insight Group. "Intelligence is what you do with that information."

One corporate investigator contacted by *The Edge Singapore* relates a case involving a wealthy individual from Norway who wanted to open a private banking account in an Asian country. Initial searches revealed nothing negative about him. But when the investigator did a local language search on the Norwegian individual, it opened a Pandora's box. Not only had the person in question been declared bankrupt in Norway, he had apparently been involved in one of the biggest frauds in his home country. The lesson learnt was that a vast amount of risk-relevant information isn't in the English language, but it exists in the public domain. To make the most of this information, staffers at business intelligence agencies are from a diverse range of nationalities. The Dubai office of such an agency is a veritable Tower of Babel, with people from 22 nationalities.

In some instances, the relevant information that corporate investigators are hired to find is actually sitting on the hard drives of their clients' own computers. According to one computer forensics analyst formerly based

CONTINUES ON PAGE 22