



fraud alert

october/november 2007

Fraud is fraud in any language
The risks of doing business in China

Don't let botnets turn you into a zombie

Surprise!
Unexpected audits are proven fraud deterrents

Fraud to watch for:
Cyber crime

Do you need employee dishonesty insurance?



McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

105 W. Madison Street, Suite 406
Chicago, Illinois 60602

Fraud is fraud in any language

The risks of doing business in China

Despite its history of communism, in recent years China has opened its markets to private enterprise. This means there are plenty of opportunities for American businesses looking for lucrative new markets. But in some cases, the desire to get rich quick coupled with rudimentary government regulations has encouraged fraud. Western companies, unfortunately, often fall victim.

If your company has Chinese operations or intends to start doing business in China, you must be certain that you understand whom you're dealing with. You also need an effective antifraud program to combat the worst elements in what some consider an economic "Wild West."

Familiar fight, new battleground

Fraud is a widespread problem for foreign businesses in China, although there are no statistics available to gauge the true extent. But the types of fraud experienced are the same as those found anywhere, as are the tools to fight them. The problem is that differences in language and culture, as well as geographic distance, make it easier for the unscrupulous to conceal fraud from Western businesses.

American companies depend on legal contracts and formalized corporate governance, but China for centuries has relied on "guanxi," or personal connections. Nepotism, therefore, is an accepted way of doing business, and handshakes seal many deals.

Lack of government oversight makes it easy for local employees to set up companies that compete with their foreign-owned employers' businesses — often using the foreign company's technology and other resources. They also may use foreign investors' assets to secure loans for themselves. This is made relatively easy by China's still-developing regulatory and auditing systems. In many cases, Chinese lenders and government authorities don't have the resources to verify assets pledged as collateral.

Other common fraud schemes in China include:

- Billing foreign investors for more than the cost of goods and services,
- Falsifying production records and selling products off the books, and
- Collusion with, or bribery involving, government officials.



Unfortunately, when books and records are thousands of miles away, in an unfamiliar language and a country where accounting standards are still evolving, it can be impossible to know whether discrepancies are a result of sloppy bookkeeping or outright fraud.

Distance breeds discrepancies

Although Western companies rate fraud as a significant risk in China, they don't appear to be taking steps to minimize the risk, according to a 2006 Ernst & Young survey. Even in markets where fraud is known to be common practice, only 32% of staff is trained to recognize the difference between facilitation fees and corrupt payments, the survey found. And 25% of employees receive no training in how to implement antifraud policies — even when policies exist and are communicated.

Many companies also face a disconnect between the antifraud policies they believe are in place and the reality as practiced by local management. Chinese managers who are compensated based on their ability to minimize costs may be tempted to hide irregularities in hours worked or workplace conditions, as well as in suspect financial dealings.

Proceed with caution

One solution is to proceed cautiously into the Chinese market. Chinese law requires foreign enterprises to partner with Chinese nationals, and it's imperative that you investigate potential partners thoroughly before embarking on a joint venture. The Foreign Commercial Service offices in U.S. consulates, trade associations such as the U.S.-China Business Council, local consulting firms and companies in China that specialize in due diligence all are sources that may be able to help.

It's also wise not to rely too heavily on local managers. Have at least one expatriate resident manager on site to monitor day-to-day activities. Also, enlist the help of independent auditors to regularly review the books rather than rely exclusively on the trustworthiness and knowledge of internal accounting personnel.

Navigating China's complex income tax rules

While foreign companies are required to partner with Chinese nationals to do business in China, the number of expatriate executives continues to increase. These high-paid employees are a lucrative source of tax income, and the Chinese government is cracking down on tax evasion.

Income tax laws continue to be updated, but they remain complex. Income is taxed every month on a progressive scale from 5% to 45%, depending on the amount of income. Someone who earns more than 100,000 RMB (\$13,000) per month, for example, pays 45%; those who make 50,000 RMB (\$6,500) per month pay 30%. Additionally, individuals who earn more than 120,000 RMB (\$15,600) per year must self-certify their annual income with a statement that includes personal as well as financial information, unless they leave the country for at least 30 consecutive days or 90 nonconsecutive days each year.

Length of residence also plays a role. Expatriates who have lived in China less than 183 days are exempt from income taxes. Those who have lived in the country 183 or more days but less than a year are subject to taxes on income earned in China only. Expatriates who have been in China more than a year but less than five years must pay tax on income earned outside the country if the payment is made by an entity resident in China for tax purposes. After five years, all income is taxable.

Because of this complexity, expatriate employees and their foreign employers should consult tax professionals to stay afloat in the ever-changing waters of Chinese income tax laws.

Finally, implement and enforce strong internal controls and antifraud policies. Because poor management-employee communication and insufficient training can hamstring even the most effective program, both should be an ongoing part of every antifraud undertaking.

Change comes slowly

The good news for foreign investors in China is that the Chinese government, particularly in the wake of recent food contamination scandals, is actively working to clean up fraud. But it's slow going for a country that's struggling to understand modern business mores and create an ethics system that will be widely accepted.

For now, Western businesses should move slowly into this market and remain vigilant once they get there. Even though China is making rapid progress, the risk of fraud remains real. ♀

Don't let botnets turn you into a zombie

Are you harboring a criminal? You could be, if you're a "zombie" linked to a botnet.

No, that isn't sci-fi speak for an alien tied to the mother ship. Zombies are computers infected with spyware and linked in sophisticated, software robot networks called botnets. According to David Dagon, a Georgia Institute of Technology researcher, the consensus among scientists is that about 11% of the world's 650 million Internet-enabled computers are hosts to botnet programs, although there is no definitive measure.

Some botnet operators use the software to launch "denial of service" attacks on companies unless they're willing to pay protection money.

What is certain is that botnets are dangerous and spreading, predominantly on Windows-based PCs. Most users don't know their computers are infected, but some of these insidious programs can cause major damage, including empty online financial accounts.

Remote control

Here's how botnets work: Code writers — often based in Eastern Europe — create malicious programs they distribute through e-mail attachments and downloads. Once the program is installed on a computer, the originator can control it through an Internet Relay Chat (IRC) system and scan for specific information. The fraudsters then can use the purloined host computer to send spam e-mails that spread viruses, as well as collect passwords, Social Security numbers, and financial and business information.

MessageLabs, a New York-based computer security firm, estimates that more than 80% of all spam

originates from botnets, and earlier this year a single Internet service provider became the first to generate more than a billion spam e-mails in 24 hours. One relatively small operator was arrested in Chicago in June. The man built bots that caused computers to freeze or reboot without notice — about 10,000 of them worldwide, federal authorities said.

A more significant arrest occurred in Seattle in May, when federal officials nabbed a man who used zombies to send millions of spam e-mails asking people to use his Internet marketing company to advertise their products. Authorities called Robert Alan Soloway one of the world's most prolific spammers, and predicted computer users could expect to see a decrease in the amount of spam as a result of his apprehension.

Breaking up business

Botnets can target critical operations and have serious consequences. The Chicago botnet operator infected computers in three hospitals and a jail health service. And a California hacker's infections reached the Naval Air Warfare Center and the Defense Information Systems Agency.




Some botnet operators use the software to launch “denial of service” attacks on companies unless they’re willing to pay thousands of dollars in protection money. These criminals order the computers in their networks to flood the resistant businesses’ Web sites with traffic, overloading them and costing the companies thousands of dollars in lost revenue.

Maintain security

Computer security programs can help protect against botnets — to a point. “Black hat” programmers are

continually refining their software to avoid detection, and so far they’re having little trouble staying ahead of the curve.

So, for now, make sure your computer security systems are up to date, and warn employees against turning them off, even briefly. Additionally, all employees should routinely monitor their “sent messages” e-mail files because one sign of an attack is outgoing e-mail the computer owner hasn’t sent. Finally, if you see signs of infestation, don’t hesitate to contact a computer forensics expert. 

Surprise!

Unexpected audits are proven fraud deterrents

Surprise audits are highly effective fraud prevention tools, but they consistently rank among the least-used defenses by businesses. Why? It may be because companies consider audits expensive, time-consuming and disruptive. In reality, surprise audits don’t have to be any of those things while remaining effective fraud deterrents.

Lower losses

According to the Association of Certified Fraud Examiners’ 2006 *Report to the Nation*, businesses that were fraud victims reported significantly lower losses and shorter-lived fraud schemes if surprise audits were part of their antifraud programs. The median loss to fraud was \$100,000 for companies that used surprise audits compared to \$200,000 for companies that didn’t. Similarly, fraud schemes on average lasted 15 months in organizations that used surprise audits, but stretched to two years in those that didn’t.

And yet, the report noted, only about 29% of reporting companies said surprise audits were a weapon in their arsenals. That’s unfortunate, because fraudsters often temporarily stop their activities when they know documents will be examined at a certain time. They’re less inclined to launch their plans if they know they can be discovered at any time. What’s more, surprise audits put employees on notice that management is serious about fraud prevention and that those who cheat will be caught.

Pennywise strategies

Fortunately, surprise audits don’t have to be expensive to be effective. Even though regular audits are comprehensive — and valuable — surprise audits can be less costly because they’re generally limited in scope or time.



These audits typically focus on higher-risk areas, such as expense reports, cash or purchasing. An audit may cover only a particular time period, be limited to a certain type of inventory or cover only a specific, susceptible account. In cases where fraud is already suspected, a surprise audit can examine only a single individual’s or department’s records. An auditor may, for example, look for inventory counts that don’t match recorded levels or receivables that are out of line with billings.

Not only do limited surprise audits allow businesses to control costs, but they can be conducted anytime, anyplace, and with any frequency. Rotating surprise audits among departments or accounts adds to their unpredictability, and thus their effectiveness as deterrents.

Communication is key


Those tempted to steal won’t be forestalled by the threat of a surprise audit if they don’t know the threat exists. Therefore, employees, managers and

executives all should be made aware that the company conducts surprise audits as part of its fraud prevention and detection program.

Likewise, when a surprise audit has been completed, employees need to be informed. By communicating results in general terms and making any follow-up actions visible, you add to the “shock and awe” effect. The communication can be anything from a short article in the company newsletter or a mention in a staff meeting to an e-mail from the president.

What’s important is that the message generate discussion and build awareness.

Part of the package

Surprise audits aren’t substitutes for a comprehensive fraud prevention program that includes regular audits, strong internal controls, segregation of duties, and fraud training and education. But used right, they can prove to be one of the most valuable components of such programs. 



raud to watch for: Cyber crime

Even when law enforcement agencies find computer evidence of wrongdoing, they may not have the expertise to analyze and preserve that evidence. High-tech training varies widely for state and local police departments across the country.

That’s about to change, the Department of Homeland Security announced recently. A national cyber crime training facility, the National Computer Forensic Institute, will be built in Hoover, Ala., to help police officers, judges and prosecutors gain the tools and skills necessary to combat computer-related crime.

Secret Service curriculum

The facility is scheduled to be completed in January 2008, and classes are to start in August of that year. Once fully operational, it’s expected to train more than 900 officials annually. Training will be based on the curriculum of the U.S. Secret Service, which is developing the program. It will include instruction on basic electronic crimes investigation, network intrusion investigation and computer forensics techniques from a staff of 18 Secret Service agents.

Along with classrooms, the building will contain a computer forensics lab with an advanced research and development area, an evidence

vault, storage and server rooms, public education exhibit space, and a conference room.

21st century technology

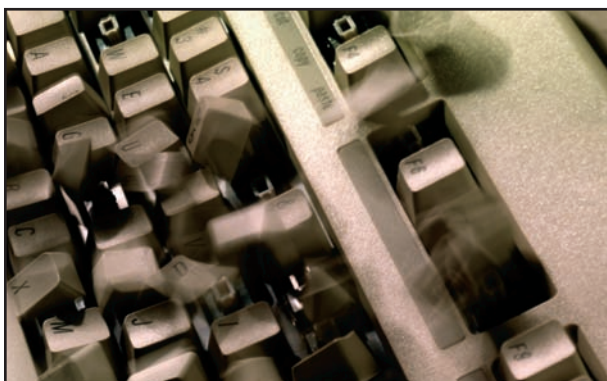
According to the Department of Justice, the FBI opened 2,135 cases of online child exploitation in 2006, compared with 113 opened in 1996. Its *Performance and Accountability Report* also notes that there’s been a substantial jump in online criminal fraud in recent years.

“The technologies that are part of everyday life in the 21st century are routinely used by criminal groups,” Homeland Security Secretary Michael Chertoff said in announcing the new training facility. “This institute will ... equip law enforcement with sophisticated skills to use the same technologies in combating criminal activities.”



Do you need employee dishonesty insurance?

Every company — whether it has 10 employees or 10,000 — is vulnerable to internal theft. The problem is so widespread, in fact, that insurance companies offer employee dishonesty coverage to protect businesses against loss of money, bonds or property due to criminal acts by employees. This can be valuable protection, but, before you buy a policy, understand what you're getting.



What it does

In addition to covering businesses against theft of money, property or securities, employee dishonesty insurance covers willful damage to property. If, for example, an irate employee smashes a computer or kicks a hole in a wall, it's likely covered. And it covers all employees. Coverage, however, is based on occurrences, so, if more than one employee is involved in a single theft, the payout is on that single occurrence.

Rates and deductibles typically depend on your business's level of risk. But separate employee dishonesty insurance policies are likely to have higher loss limits and more customized coverage than is available with coverage offered as part of a total business insurance package.

What it doesn't do

Employee dishonesty insurance isn't liability insurance. It covers only property your business owns, holds for others or is legally liable for. It usually doesn't cover theft or damages caused by employees of businesses that provide services to your company, although some vendor employee dishonesty coverage is available. A manufacturer that contracts

for cleaning services, for example, won't be compensated if a cleaning employee pilfers from their supply room — even if the cleaning company has employee dishonesty insurance.

Employee dishonesty insurance also won't cover loss of intangible assets such as trade secrets or electronic data. Thus, if one of your employees sells proprietary information to a competitor, you aren't covered for the loss.

Also not included in employee dishonesty insurance coverage are:

Unexplained disappearance of property. Regardless of how certain you are that someone stole something, it isn't covered unless you can prove it.

Loss of employees' property. Coverage applies only to property owned by your business.

Damage covered by another insurance policy. You can't expect to be paid twice for the same loss.

The burden of proof for employee dishonesty claims is solely on the policy owner. Insurance companies will pay claims only if there is conclusive proof that employee theft caused a loss.

Finally, employee dishonesty insurance isn't a substitute for a fidelity bond if a bond is required by a funding source or other contractual agreement. Federal Bonding Program bonds, originally intended to encourage employers to hire ex-offenders and other hard-to-place applicants, reimburse employers with no deductible for loss due to employee theft.

Consider your options

Your business can cover theft losses in a number of ways, including with commercial general liability policies (which may require riders) or with fidelity insurance, which varies in coverage and may not always be enough to cover all losses. Consider all the options for limiting employee theft losses before you decide whether employee dishonesty coverage is appropriate for you. Also keep in mind that comprehensive internal controls can vastly reduce your risk. ♪

McGOVERN & GREENE LLP

Certified Public Accountants & Consultants

Specialists in Fraud Examination and Litigation Services

If a business hasn't yet been a victim of fraud, it's been fortunate. According to the Association of Certified Fraud Examiners, fraud costs businesses in the United States billions of dollars every year. Small businesses are especially vulnerable because they often do not have controls in place to reduce the likelihood of fraud.

This is where McGovern & Greene LLP can help. Our firm specializes in helping corporations, attorneys, lenders, law enforcement and governmental agencies analyze financial records and contracts, identify and prevent fraud, recover and analyze evidence, and provide expert testimony in all of these matters. Our highly-experienced team of professionals includes certified fraud examiners and certified public accountants that are experts in the fields of fraud examination, forensic accounting, computer forensics, damage calculations, business valuations and audit services.

Our professionals can assist you in a wide range of matters, including:

- Fraud Examination
- Financial Investigations
- Forensic Accounting
- Asset Recovery
- Internal Audit Services
- Computer Forensics
- Training & Seminars
- Healthcare Audit
- Business Valuation
- Litigation Services
- Government Contracts
- Economic Damages
- Intellectual Property
- Contract Claims
- Construction Audits
- Electronic Discovery
- Profit Recovery
- Due Diligence



Craig L. Greene, CFE, CPA

An internationally recognized public speaker, Craig has lectured on topics involving fraud and its detection to auditors, investigators and attorneys. He is a faculty member of the Association of Certified Fraud Examiners and Institute of Internal Auditors.

Craig works as a consultant and expert witness for major corporations, law firms, law enforcement and governmental agencies on cases involving allegations of fraud and misrepresentation. Craig is frequently quoted in major newspapers and publications throughout the U.S.

We welcome the opportunity to discuss your needs and answer any questions you might have about our fraud examination and litigation services.

Please contact us at 312.419.1961 or visit us at www.mcgovernngreene.com and let us know how we can be of assistance.

McGovern & Greene LLP
105 W. Madison Street, Suite 406
Chicago, Illinois 60602

