# CYBERRISKS&LIABILITIES_
NEWSLETTER

**October / November 2013**

## IN THIS ISSUE



## Employee Management to Reduce Fraud

One of the biggest threats to your business may come from inside it. Staff fraud—fraudulent acts committed by employees for monetary gain—is potentially disastrous for your company. Worse, it is under-reported and on the rise. The typical organisation victimised by staff fraud loses 5 per cent of its annual revenue due to its employees' fraudulent acts, according to a recent report by the Association of Certified Fraud Examiners. With businesses relying more on technology, staff fraud can now occur anytime and anywhere.

Types of staff fraud include embezzling, insider trading and forging checks, expense reports and supplier invoices. Most of these fraudulent activities can be perpetrated online. Although staff fraud may seem difficult to detect until it's too late, implementing a mutli-pronged employee management programme can lower many of your company's staff fraud risks.

Combating staff fraud starts with identifying the signs. Certain conditions are present when an employee commits fraud; these three conditions are known as the 'fraud triangle':

- **Motive.** Defrauders must have a motive to commit fraud, and this motive is often pressure. This can come from feeling too much stress to meet deadlines at work, or trying to live a lifestyle that is beyond the defrauder's means. Outside problems such as a gambling addiction can also motivate defrauders.

- **Opportunity.** If your anti-fraud measures are too lax, you present an opportunity for defrauders. Even if the perpetrator is financially stable, the opportunity might be too tempting to ignore. Make sure your systems are properly password protected and that only necessary employees have access to financial documents.

- **Rationalisation.** Defrauders must be able to justify their actions. If employees sense some sort of wrongdoing on the company's part, they might be able to justify fraud.

Implementing fraud prevention measures is easier than identifying already-committed fraud. To start, make sure you perform a pre-employment screening on all potential employees. Let these employees know there are policies on cyber fraud and cyber theft in place. Because workplace fraud is much more likely to be detected by anonymous tips, establish a tip line that employees, clients or suppliers can use to report cases of fraud.

If you run a small business, avoid granting unsupervised leadership to your employees—this encourages fraud. Split up the duties among a larger pool of employees to decrease the likelihood of fraud.

No matter the size of your business, do not get complacent. Any employee can commit fraud. Conduct random audits with an accountant to maintain effective internal financial controls. Ensure your employees are satisfied with their work and the company. Reward them for doing well. A satisfied employee is happy and less likely to commit fraud.

Crendon Insurance Brokers

# Recent Syrian Cyber Attacks Highlight Need for Protection

The recent cyber attacks by the Syrian Electronic Army (SEA) call attention to businesses' vulnerability to such crippling cyber breaches. The SEA is a group of hackers and activists who seek to counter what they call the 'fabricated news' disseminated by Arab and Western media. The BBC, Associated Press and Financial Times have all been victims of malicious cyber attacks that jeopardised data security and business integrity. Such attacks cost large businesses an estimated £450,000 to £850,000 per breach.

Follow these 10 steps to protect yourself against the ever-growing threat of cyber attacks.

- Develop a mobile working policy and train staff to adhere to it.
- Produce user security policies dictating acceptable and secure use of your organisation's systems.
- Establish an incident response and disaster recovery capability.
- Outline an effective governance structure and determine your cyber risks.
- Limit employee cyber privileges and monitor user activity.
- Create a policy to control all access to removable media.
- Monitor all systems and networks and continuously analyse activity logs.
- Apply security patches and ensure the continued secure configuration of all information and communication technology.
- Scan for malware across your organisation.
- Test security controls and filter out unauthorised access and malicious content

## Fine for Aberdeen City Council homeworking arrangements

The Information Commissioner's Office (ICO) ordered Aberdeen City Council to pay a £100,000 penalty after a data breach resulted in sensitive information being published online. A council employee accessed the information from her home computer, but forgot about her machine's file transfer program, which automatically uploads all downloaded files to a website. The files, which included details about children's welfare and alleged criminal offences, were left online for about four months until another council employee spotted the documents through an unrelated online search. The ICO declared the council had no relevant homeworking policy and had insufficient measures to protect the sharing of sensitive information.

## Personal data released online leads to monetary penalty

A £70,000 penalty has been served to Islington Borough Council after personal and medical details of over 2,000 residents were released online via the What Do They Know (WDTK) website. WDTK enables individuals to request information from public authorities in response to a freedom of information inquiry. The council released three spreadsheets related to an inquiry into its Housing Performance Team to WDTK, failing to notice that the spreadsheets contained details from residents' housing applications. The ICO's investigation found that the council was sluggish in responding to the breach and had scant data protection policies in place.

## Prosecution for probation officer who released victim information

A probation officer was prosecuted and fined £150 after she revealed a domestic abuse victim's name, address, date of birth and more to the alleged attacker. The officer believed the alleged attacker already knew the information. The distressed victim called the police the day after the information was illegally provided, claiming that the perpetrator unlawfully attained the victim's new address. The victim subsequently severed all contact with the police, convinced they could not be trusted. The investigation against the alleged perpetrator was then dropped, due to the victim's lack of cooperation.

CYBERRISKS&LIABILITIES_
NEWSLETTER

**Crendon Insurance Brokers Ltd**
11 Greenfield Crescent
Birmingham, West Midlands, B15 3AU
0121 454 5100
www.crendoninsurance.co.uk