WHAT IS THE INSIDER THREAT?

White paper created by The Security Company

January 2013
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction: What is the Insider Threat?</td>
<td>3</td>
</tr>
<tr>
<td>Types of Insider Fraud</td>
<td>4</td>
</tr>
<tr>
<td>What makes employees a threat?</td>
<td>5</td>
</tr>
<tr>
<td>What are the most common threats?</td>
<td>5</td>
</tr>
<tr>
<td>Non-deliberate insider threats</td>
<td>6</td>
</tr>
<tr>
<td>How can you identify the threat and protect your organisation?</td>
<td>7</td>
</tr>
<tr>
<td>Sources of further advice and information</td>
<td>8</td>
</tr>
</tbody>
</table>

## Appendix

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sources used in the preparation of this report</td>
<td>9</td>
</tr>
</tbody>
</table>

## About The Security Company

The Security Company is a leading provider of creative employee security awareness programmes. We deliver best in class security education programmes that minimise organisational risks and strengthen business. We do this by creating a dynamic culture of security awareness; educating and empowering your employees and alerting them to risks and their personal responsibilities. Founded in 1997 by Martin Smith MBE, we are recognised as being at the forefront of the ‘human factors in security’ debate.
Introduction: What is the Insider Threat?

While most staff within an organisation are trustworthy and honest, there is the ever present threat from insiders doing the wrong thing: executives, employees, independent contractors, temporary staff members and trusted third parties. The threat can be either deliberately malicious, as in fraud; or come from negligent behaviour, fostered by a lack of training and poor policies.

Fraud costs business billions each year, with current fraud trends indicating that professional criminals are targeting business and attacking it from within.

Some fraud statistics:

- 85% of reported fraud is committed by people within the organisation
- A typical organisation loses approximately 5% of its annual revenue to staff fraud
- Fraud cost the UK economy £38.4 billion in 2010
- 314 major fraud cases worth £100,000+ were heard in the Crown Court in 2010, totalling £1.374 billion
- 372 reported cases of fraud in 2010 were in excess of £50,000, worth £1.4 billion
- CIFAS research has shown that staff fraud has increased by over 40% in the last three years
- Large organisations employing more than 80,000 people can expect to dismiss in the region of 100–150 members of staff a year for fraudulent activity (CIFAS)
- 15% of CVs contain at least one discrepancy in the form of dates, directorships, academic qualification and bankruptcy
- 330 cases of staff fraud were identified during 2010

Analysis of frauds recorded on the CIFAS Staff Fraud Database during the first half of 2012, compared with 2011, has revealed the following:

- A 52% overall increase in the number of insider frauds recorded
- Precarious economic and employment conditions demonstrated by the 24% increase in dishonest actions by staff to gain a benefit, with fraudulent attempts to gain employment more than doubling
- A 53% surge in theft of customer data (the most valuable data) by an employee
Types of Insider Fraud

Insider-enabled fraud is wide ranging, here are some examples:

- Fraud against the organisation, often described as ‘staff fraud’, ‘employee fraud’ or ‘internal fraud’. For example, when an employee submits a false expenses claim.
- Fraud against the organisation when the insider colludes with an outside accomplice(s). For example; a finance manager authorising payment of a false invoice from a supplier for non-existent works in exchange for a ‘kickback’ payment.
- Fraud against an outside entity. For example, an employee stealing a database containing personal details of customers, which is used by a criminal gang to obtain money, credit, goods or services fraudulently from other organisations, such as bank accounts, loans and mobile phone contracts.

Of those who said their private sector organisation had been a victim of fraud in the past year, 22.6 per cent said they had suffered at least one insider-enabled fraud.

Fraud can take place at any time during the employee lifecycle:

“Consider the lifecycle of your employees. Fraud can take place: pre-employment, during employment and post-employment.”

Pre-employment; lies may be considered acceptable when jobs are hard to come by:

- Falsification of academic records or qualifications
- Altering employment history or dates
- Undisclosed directorships
- Undeclared County Court Judgements or bankruptcy

During employment; dishonest behaviour:

- Account (customer) fraud
- Obtaining or disclosing personal data
- Theft or deception to obtain a benefit
Post-employment; individuals may be working for a competitor; have a grievance and lack loyalty; and may have had access to significant and potentially damaging information:

- Unauthorised access to systems
- Disclosing personal or commercial data
- Denial of service attacks

Many insider crimes probably go unreported either because they have not been noticed or because the organisation does not want to risk exposure to damage to reputation. CIFAS estimates that only 27% of staff fraudsters were reported to the police in 2010.

What makes employees a threat?

The temptation to commit fraud may be increased in times of recession; with rising living costs, high levels of debt and the worry of job losses – though there is some evidence that insecurity improves people’s behaviour as they value their job. Redundancy or grudges such as low pay or being passed over for promotion, may give rise to feelings of revenge, which is particularly dangerous if network access has not been removed. There may also be increasing pressure of work. However, it should be remembered that not all insider threats are deliberate and criminal.

The most common cause of staff fraud is greed – to fund a lifestyle they could not otherwise afford; to support a habit such as gambling; or to pay off debts. In many cases they will continue to undertake fraud after the arrears have been successfully cleared.

What are the most common threats?

According to the report CIFAS Staff Fraudscape 2011, the most common threat was staff attempting, fraudulently, to obtain an advantage by theft or deception. For example, a high street bank cashier stealing cash from a customer who was depositing their cash into their account. Furthermore, the compromise of customer or payroll data to facilitate fraudulent activity by third parties still continues to be a significant threat to the financial services industry and public bodies that hold large amounts of personal data about citizens. This will also be the case for organisations in other sectors of the economy and is due to the involvement of organised crime, the potential and current financial losses, the possible impact on customer confidence and the number of incidences. However, all types of staff fraud have the potential to severely damage an organisation, particularly its reputation.

Although an element of greed is present in the vast majority of staff fraud cases, employees are known to commit fraud according to three variables:
Opportunity - organised criminals and a growth in personal debt has provided a more direct motivation and more obvious source of pressure than previously existed. Generally, staff fraudsters will typically be motivated by financial gain, which may or may not be linked to collusion with organised criminals or personal associates.

Motivation/pressure - targeting by organised criminals and a growth in personal debt has provided a more direct motivation and more obvious source of pressure than existed previously.

Integrity/rationalisation - the infiltration of organisations by criminals when combined with a high staff turnover, reduced loyalty, relatively low pay compared with the national average and the perception of fraud being a ‘victimless’ crime with little chance of being caught, means that members of staff will increasingly rationalise the crime they are committing.

The CIFAS Staff Fraud and Dishonesty 2012 Report said that there was no common profile of a staff fraudster, but identified that the fraudster was typically:

- Male or female with an average age of 30
- Working in retail or the finance department
- Working at the organisation for more than five years
- Motivated by greed or work pressures

The insider threat may also be facilitated by:

- Use of temporary and/or agency staff
- Insufficient vetting of prospective employees
- Call centres
- Corrupt employees moving between companies
- Employees targeted by organised criminals
- Corrupt employees coercing other employees
- Poor management practices and weak organisational culture
- Ineffective grievance processes for employees
- Lack of a strong security culture
- Inadequate personnel security measures during pre-employment screening and after recruitment

Non-deliberate insider threats

Not all insider threats are deliberately fraudulent. Without effective training and policies, human error and inattention can expose the organisation to a number of risks. Malware infection can occur despite perimeter defences such as firewalls, anti-virus and intrusion prevention systems if staff fall victim to:

"UBS uncovered unauthorised trading producing losses of $2.3bn (£1.5bn) in 2011."
Social engineering and phishing. For example, luring computer users into giving up passwords; or to open otherwise innocuous-looking email attachments that contain malware. The RSA incursion in the US was the result of an email sent to selected employees with “2011 Recruitment Plan” in the subject line; and an attached infected spreadsheet.

“Spear phishing,” involves infected messages sent to selected individuals that appear to be from a trusted source. These attacks take a long time to develop, but when they succeed perpetrators can stay undetected inside an organisation’s network for weeks, months or even years while collecting data or sabotaging assets.

Malware infection, such as the Stuxnet worm, of supposedly airtight internal networks from a USB stick used unwittingly by an employee.

How can you identify the threat and protect your organisation?

- In 2011 Swiss bank UBS uncovered unauthorised trading by a member of staff, Kweku Adoboli, producing losses of some $2.3bn (£1.5bn). Confidence in the bank’s reputation was clearly harmed, with an immediate 7% fall in its shares.
- In 2008 the French bank Société Générale revealed that rogue trader Jérôme Kerviel had lost the bank £7bn.
- In 1995 rogue trader Nick Leeson lost £800m and destroyed Barings Bank whilst working as chief trader for Barings Futures in Singapore.
- Adoboli, Kerviel and Leeson’s co-workers and bosses seemingly failed to recognise that there was a problem and to step in to prevent the losses incurred as a consequence. Nobody wants to believe their friends, employees or colleagues could be defrauding them.
- Adoboli’s had a 420-strong list of friends on Facebook who did not recognise from his updates that he was under pressure. When the market fell steeply he posted: “Can we shut down global markets for a week so everyone can just chill out?” After a series of increasingly desperate posts his last message said: “Need a miracle”.
- Although most fraud is discovered through technical monitoring, internal controls and audit, we must look out for and recognise any signs that something might be wrong with someone we work with. Co-workers are likely to know the habits of others and be more sensitive to suspicious behaviours and changes in personality which could indicate an insider threat. Encourage a culture of “see something, say something” so that if staff recognise uncharacteristic behaviour in their colleagues, they subsequently inform the relevant people. Have in place a well communicated and simple to follow reporting process in order to support this as a method of prevention.

Defend your organisation from insider crime by:

- Effective supervision – set the tone from the top
- An anti-fraud strategy, tailored to the needs of the particular organisation
- Listening to staff concerns and encouraging them to speak up
- Looking for weaknesses in controls and systems
- Technical controls such as server room audit trails and disabled USB access to prevent data theft
- Effective pre-employment screening
- Disabling access privileges on termination of employment
- Be honest – report fraud, prosecute if necessary and give truthful references for employees
Avoid

- Complacency
- Passing the buck (someone else’s problem)
- Failure to supervise
- Assuming that former employees will remain loyal to the organisation

To summarise, “In a challenging environment of constantly developing technologies, economic hard times and a scarcity of employment, organisations who do not take this threat seriously must recognise that the dangers they face in terms of their financial well-being, ability to operate legally and their reputation are immense.” CIFAS, August 2012

Sources of further advice and information

Useful sources of information on the insider threat can be found at:

- Pre-employment screening factsheet [FAP] — Available free from [www.fraudadvisorypanel.org](http://www.fraudadvisorypanel.org)
- HMG baseline personnel security standard [Cabinet Office] — Available free from [www.cabinetoffice.gov.uk](http://www.cabinetoffice.gov.uk)
- Tackling staff fraud and dishonesty: managing and mitigating the risks [CIFAS & CIPD] — Available free from [www.cifas.org.uk](http://www.cifas.org.uk)

Appendix

Sources used in the preparation of this report:

Verizon Data Breach Report 2012
CIFAS Staff Fraudscape May 2011
CIFAS Staff Fraud and Dishonesty – Mitigating risk 2012
NFA Annual Fraud Indicator 2011 and 2012
KPMG Fraud Barometer 2011
Kroll Global Fraud Report 2010
ACFE Global Fraud Survey 2010
The Security Company SASIG March 2011
The British Computer Society
Contributions

Key contributions to the white paper were made by:

Ruth Pooley,
Researcher and Content Editor,
The Security Company

Bernadette Palmer,
Head of Communications,
The Security Company

Contacts

If you would like to discuss any elements of the white paper, and/or find out more about how The Security Company can make a difference within your organisation with regards to security and risk prevention, contact our team today.

Martin Smith MBE
Chairman and Founder
+44 (0) 1234 708456
martin@thesecurityco.com

Lisa Spriggs
Marketing Executive
+44 (0) 01234 707024
lisa.spriggs@thesecurityco.com

This white paper has been prepared by The Security Company (International) Limited (TSC). It is for general guidance on matters of interest only, and does not constitute professional advice. You should not act upon the information contained in this report without obtaining specific professional advice.

This white paper contains information obtained or derived from a variety of sources [as indicated within the report]. TSC has not sought to establish the reliability of those sources or verified the information so provided. Accordingly no representation or warranty of any kind (whether express or implied) is given by TSC to any person as to the accuracy or completeness of the information in this white paper.

TSC accepts no duty of care to any person for the preparation of the white paper. Accordingly, regardless of the form of action, whether in contract, tort or otherwise, and to the extent permitted by applicable law, TSC accepts no liability of any kind and disclaims all responsibility for the consequences of any person acting or refraining to act in reliance on the white paper or any information contained in the white paper or for any decisions made or not made which are based upon this report or information therein.

The Security Company (International) Limited
Dean Court, Upper dean, Huntingdon, Cambridgeshire, PE28 0NL
Tel: +44 (0) 1234 708456
Email: enquiries@thesecurityco.com
Website: www.thesecurityco.com