TenInsight

TenIntelligence

www.tenintel.com | October 2018 | Issue 4

What's your vision?

Integrity should be at the core of every organisation's risk, compliance and anti-fraud programme. In this edition, we focus on the Financial Reporting Council's recent Good Corporate Governance Code highlighting how governance should be implemented, reported and measured by listed companies both in the UK and abroad.

The key message from the Code is to be transparent. Demonstrating good governance not only reinforces an organisation's reputation but provides it with opportunities over others.

Even if you are not part of a listed company, the Code highlights useful areas for SMEs to consider on improving their journey to integrity.

With the Code in mind, we also share some key red flags, highlighted by the Association of Certified Fraud Examiners (ACFE), of officers, directors and employees who commit fraud against an organisation from within – the very people who were entrusted to protect its assets and resources. Can you spot any red flags in your organisation?

GDPR continues to be a hot topic, even though the legislation was introduced back in May. Richard Bell, our Privacy & Security Director, reviews several common themes clients have highlighted since the introduction of the new rules.

On the subject of transparency, we recently asked ourselves what integrity means to TenIntelligence and what our vision is.

We defined our vision "to be the playmaker in our field; an investigation and protection consultancy, recognised for our diligence, excellence and integrity. Our intelligence – your assurance".

What's your vision?

Neil Miller
CEO, TenIntelligence

ACFE – 2018 Global Report to the Nations

The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organisation and premier provider of anti-fraud training and education. The ACFE regularly conducts a global fraud study with insightful findings which can help organisations with their fraud risk management.

This year, the ACFE's 2018 Report to the Nations on Occupational Fraud and Abuse provided analysis of 2,690 cases of occupational fraud that were investigated by Certified Fraud Examiners, between January 2016 and October 2017. The fraud cases in the study came from 125 countries throughout the world, providing a truly global view into occupational fraud.

Among the various kinds of fraud that confront organisations, occupational fraud (a fraud committed against the organisation by its own officers, directors, or employees) is likely the largest and most prevalent threat.

It constitutes an attack against the organisation from within, by the very people who were entrusted to protect its assets and resources.

The Primary categories of occupational fraud

Asset misappropriation

Of the three primary categories of occupational fraud, asset misappropriation is by far the most common, occurring in 89% of the cases in the study. However, they are also the least costly, causing a median loss of £90,000.

Asset misappropriation types:
Theft, skimming, forgery, invoice fraud, payroll fraud, expense fraud, fund misuse

Corruption

Corruption schemes are the next most common form of occupational fraud; 38% of the cases in the study involved some form of corrupt act. These schemes resulted in a median loss of £200,000 to the victim organisations.

Corruption types:
Conflict of interest, bribery, illegal gratuities, kickbacks and extortion

Financial statement fraud

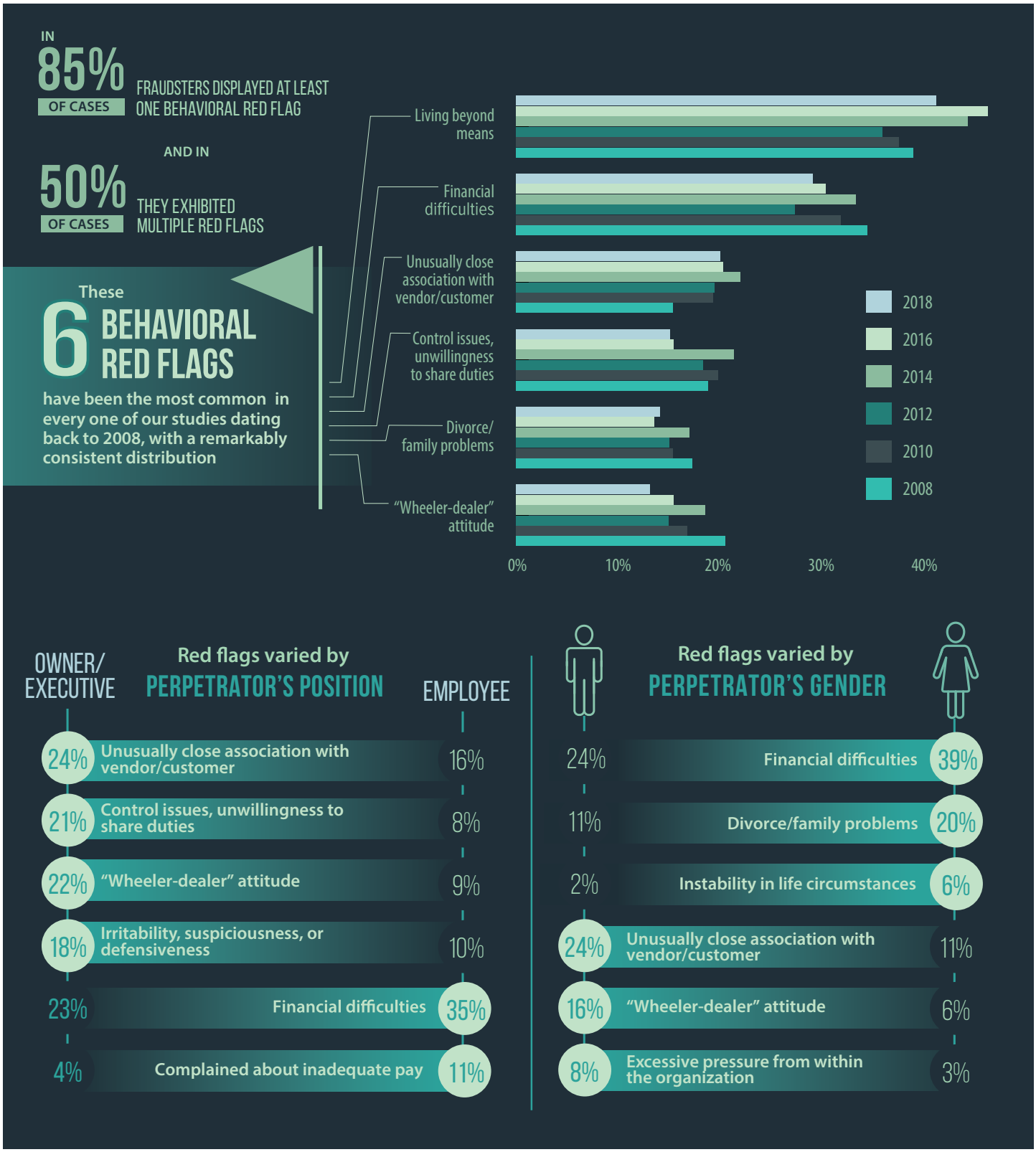
The least common, but most costly, form of occupational fraud is financial statement fraud, which occurred in 10% of the cases and caused a median loss of £620,000.

Financial statement fraud types:
Fictitious reporting, concealments, overstatements, timing differences, improper asset valuations

The 'Red Flags' of fraud

Understanding and recognising the behavioural red flags displayed by fraud perpetrators can help organisations detect fraud and mitigate losses.

Living beyond means and financial difficulties have been the most common red flags in every ACFE study since 2008. In 85% of the cases reported (see graphic on page 2), fraudsters displayed at least one behavioural red flag and in 50% of cases, the fraudsters exhibited multiple red flags. *Continues on next page...*



www.acfe.com/report-to-the-nations/2018

What we can do for you

Neil Miller, our CEO, is a Certified Fraud Examiner and gives the following advice:

"We have successfully provided clients suffering multi-million-pound frauds, corruption cases and intellectual property infringements with the evidence and intelligence required to win their cases and help recover their assets. Once a suspicion of fraud has arisen, don't panic but act quickly. Seize the initiative by developing a course of action. Analyse the available evidence and circumstances surrounding the suspicion, retain accurate records, develop a fraud theory and set out your objectives in an investigation plan."

New UK Corporate Governance Code

In July 2018, a new edition of the UK Corporate Governance Code was released by the Financial Reporting Council, whose mission is to promote transparency and integrity in business. The Code is applicable to all companies with a premium listing in the UK or elsewhere.

Companies listed on stock exchanges will be required to adapt and implement a range of different Principles which will be applied to those companies with accounting periods beginning on or after January 1st 2019; although, companies can choose to adopt the new Code earlier.

The listing rules require companies to make a statement of how they have applied all 18 Principles, articulating what Provisions (there are 41 Provisions in total) have been taken and the resulting outcomes. Accurate and transparent reporting will help investors with their evaluation of company practices.

There are several Principles and accompanying Provisions that have been amended, which companies will need to adopt. We have summarised these below:

Board leadership and company purpose

The Board should implement long-term sustainability by establishing the company's purpose, values and strategy. These should be well resourced, controlled and measured to meet its responsibilities to the company's shareholders, stakeholders and workforce.

Division of responsibilities

The Chairperson is responsible for the overall effectiveness of the Board and ensures that the appropriate executive and non-executive directors receive accurate, timely and clear information. The roles of each Board Director should be well defined with a clear division of responsibilities between the Board and the management of the company.

Composition, succession and evaluation

Appointments to the Board and their succession plan should be subject to formal and transparent procedures based on an individual's skills, experience and knowledge. The Board and its committees should promote individuals with a diversity of gender, social and ethnic backgrounds as well as personal strengths.

Audit, risk and internal control

The Board is required to implement formal and transparent policies and procedures, to ensure independence and satisfy the effectiveness of its internal and external accounting obligations. The policy and procedure framework must also include the nature and extent of the principal risks the company faces and how it intends to mitigate these risks to achieve its long-term sustainability.

Remuneration

A formal and transparent procedure for determining executive remuneration should be implemented. Executive and non-executive remuneration should be aligned with the company's purpose and be clearly linked to the successful delivery of the company's long-term objectives. No director should be involved in deciding their own remuneration.

The 2018 Code and its Principles are supported by a revised Guidance on Board Effectiveness, which Board Directors are encouraged to read in conjunction with the Code.

The full UK Corporate Governance Code is available for free from the Financial Reporting Council website www.frc.org.uk

GDPR: What we've learnt so far

Following its introduction back in May, we are now some four months into the General Data Protection Regulation (GDPR) and it remains a hot topic with clients.

Whilst the furore of the May deadline has been and gone, does the appetite to become or even remain GDPR compliant still exist?

Since May, our team has been spending time ensuring our clients' preparations are well executed and helping them provide a clear picture of where their data exists. The interesting aspect to this is that no matter the organisation, or goals associated with it, they all have personal data that requires protection of varying degrees. Some make their business about the personal data, some need the data to enable business and some have it to operate a business.

GDPR compliance is an ongoing process and will require an ongoing effort. Organisations have had two years to prepare for the regulations and yet many have only just started their compliance journey. While this is not ideal, it is likely that the Information Commissioners Office (ICO) will not tolerate non-compliance.

So what have we seen so far? Several common themes have emerged that we thought would be useful to share:

Breach and incident reporting

The processes to support the identification of and subsequent reporting of a breach, loss or incident to the ICO have not been robust enough to report in a timely manner. That – coupled with a lack of coordinated involvement, role responsibility and a "what happens if" plan – has put organisations at risk of falling at the first hurdle when reporting within the mandatory 72 hours deadline.

Data Protection Officer

(appointed internally or externally)

Small, medium or large organisations have all found this area challenging. Articles within the GDPR state that an independent person should be appointed and have responsibility for managing the protection of data and acting on the organisation's behalf in regard to all matters relating to data protection. This single resource can be quite draining, expensive and doesn't often exist within organisations. Moreover, there is confusion around ownership of all data protection activity, both at operational and board level. *Continues on next page...*

Third party assurance

Most organisations were successful in identifying where their personal data is, during transit, at rest and when in use. However, some have forgone responsibility for the data once it is handed over to a third party. This is simply no longer acceptable and is a dangerous weakness in the controls that should be in place. Upon review, several clients did not have contractual requirements outlining the security and protection standards afforded to personal data found in service agreements.

Many clients had not considered due diligence within their supply chain and the use of third parties to ensure compliance.

Myth buster: Technology is not enough

Technology alone cannot solve your compliance questions, lawyers can certainly position you legally and assist with those aspects within the regulations such as the bases for processing and contractual agreements. Insurance companies can offer some level of protection, but only the organisation itself can do the real work required: it is not easy but it is achievable.

Richard Bell, our Privacy & Security Director, said: "We work closely with decision-makers assisting them with the implementation of data privacy measures. We help audit their compliance obligations and resiliency by testing systems, processes and infrastructure."

Our team offers support and assists with an organisation's GDPR compliance, cyber-security and incident response measures, including:

- A complete review and/or developing a framework of policies and procedures needed to ensure GDPR compliance
- Provide a plan for Data Protection or Privacy by Design documentation
- Implement a regular review of security access and controls to ensure privacy and security of personal data
- Help organisations develop a staff training and awareness programme
- Provide leadership support and a business focal point for training to all staff on GDPR matters
- Support the regular testing regime of breach and incident response including specific development of bespoke desktop and playbook exercises to test decision-making procedures
- Develop a communication plan for internal and external messaging to clients and staff, offering specific support for press and media handling
- Conduct information and security audits across the business to review, identify and assess known and unknown risks, including site visits, physical security reviews and provide an assurance opinion
- Ongoing virtual support and communication and reporting on the current state of the organisation
- Dedicated data protection experts who can provide real-time assurance through the provision of appropriate reporting mechanisms

Updates from our Dubai office

Raids in the UAE

Since May 2018, TenIntelligence has seized more than 300,000 counterfeit products from the UAE market. One of these seizures was conducted with the outstanding support of Sharjah CID and was the largest haul that the client has had in the region. The products seized included; counterfeit laptop power adapters, laptop batteries, LCD screens, smart phone batteries and chargers. The health risks that these products pose, in the event that they explode when in use and cause serious harm to the individual, was stressed to law enforcement authorities.

Dubai office is expanding

We would like to welcome our latest member to the TenIntelligence team – Ahmed Elodimi. Ahmed has over five years of experience in anti-counterfeiting investigations in the UAE and comes with a great wealth of knowledge of the market. He is certainly keeping us busy on enforcement action!

Brand owner attends raid

TenIntelligence hosted a client for two full days, arranging meetings with law enforcement officials and provided an insight into how local raid actions take place. We conducted two raids: one in Jebel Ali Free Zone (Dubai Police) and the other on mainland Dubai (Dubai Economic Department). The combined seizures from these two raids equated to 10,500 pieces.

Interpol Conference 25-26 September 2018

TenIntelligence attended the International Law Enforcement IP Crime Conference led by Interpol and one of our partners, Underwriters Laboratories (UL), in Dubai this month. We provided support for UL, presenting to all UAE law enforcement officials training on how to identify UL counterfeit products in the market.

Due Diligence | Investigations | Brand Protection | Privacy

Contact Us

UK
+44 (0)20 3102 7720
info@tenintel.com

MIDDLE EAST
+971 (0) 4333 4669
dubai@tenintel.com

@tenintelligence