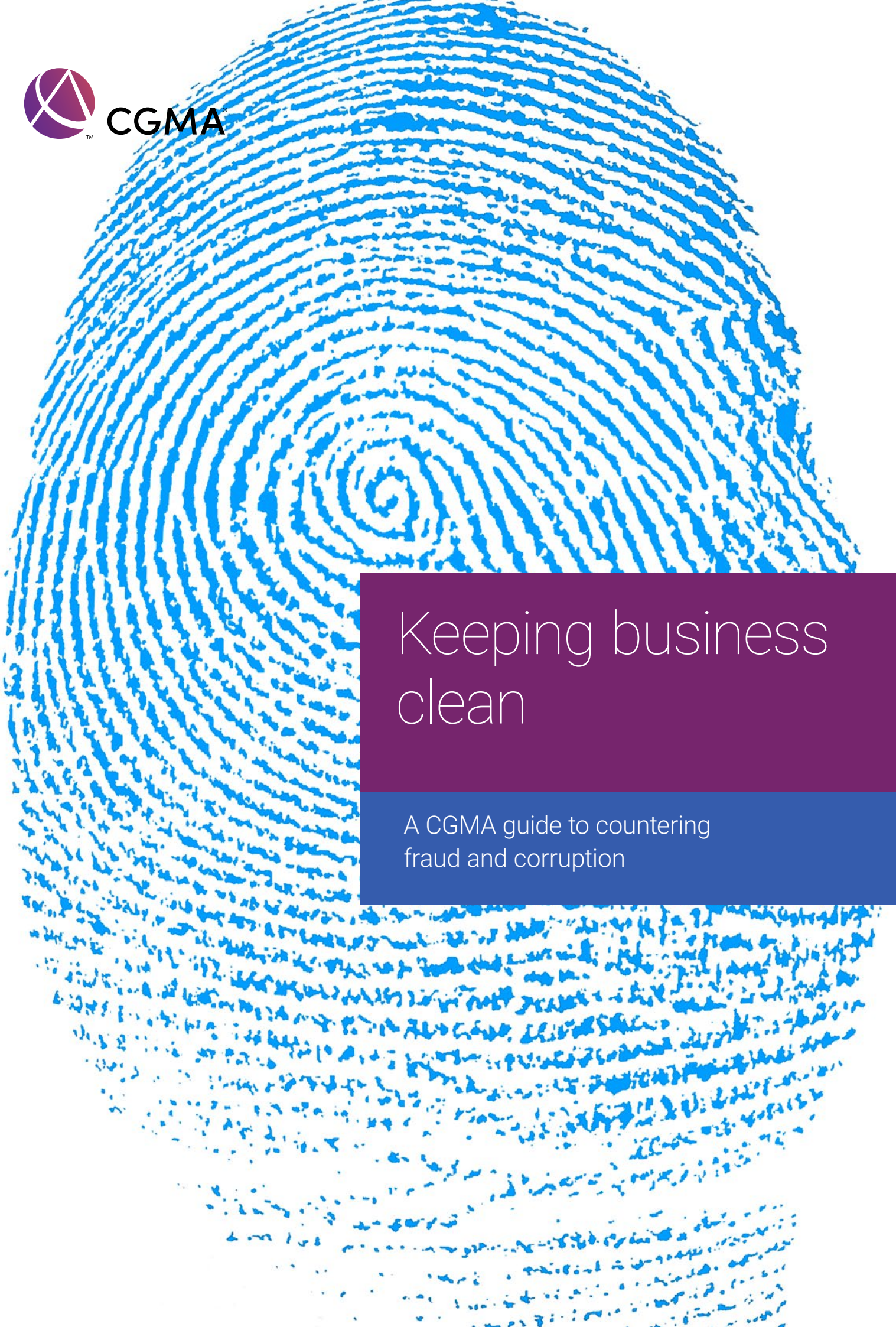


CGMA

Keeping business clean

A CGMA guide to countering fraud and corruption

Chartered Global Management Accountant (CGMA®)

CGMA is the most widely held management accounting designation in the world. It distinguishes more than 150,000 accounting and finance professionals who have advanced proficiency in finance, operations, strategy and management. In the U.S., the vast majority are also CPAs. The CGMA designation is underpinned by extensive global research to maintain the highest relevance with employers and develop competencies most in demand. CGMA designation holders qualify through rigorous education, exam and experience requirements. They must commit to lifelong education and adhere to a stringent code of ethical conduct. Businesses, governments and nonprofits around the world trust CGMA designation holders to guide critical decisions that drive strong performance.

cgma.org

Contents

* Also see our accompanying briefing, Anti-Corruption landscape 2017, co-produced with Transparency International and featuring their Global Corruption Perceptions Index and overviews of key global legislation including FCPA and the UK Bribery Act.

Authors

Tanya Barman,

Associate Director, Ethics

Nancy Marc-Thrasybule,

Lead Technical Manager,
Management Accounting
Professional Unit,
The Association of International
Certified Professional Accountants

1 Introduction and overview: fraud and corruption in the global landscape

Despite the many advances in awareness movements, legislation and evident public protest, fraud and corruption continue to blight governments, businesses, civil society and wider economies. Professional accountants, with their in-depth training, ongoing professional development and commitments to their Codes of Ethics and related financial standards, play a critical role in both assessing fraud and bribery risks and tackling issues that come to light.

The topic of fraud and corruption covers a huge landscape from unethical business practices such as bribery and criminal activities to an array of fraudulent financial schemes including money laundering, financial statement misrepresentations and asset misappropriations. The increased level of risk that comes with these weaknesses has different implications depending on the size of organisation, sector and geography. With rapid technological advances, the methods of corrupt practices have evolved and take many forms. Cybercrime has become a prevalent term and the multiple guises of it, including executive impersonation as featured in this briefing, can impact any organisation. Conversely, technology has a huge role to play in countering fraud and corruption through, for example, advanced forensic software.

This briefing highlights some of the recent global developments and trends to useful resources and insights from across the Association of International Certified Professional Accountants (AICPA, CGMA and CIMA) and other leading providers of anti-corruption and fraud materials.

The World Bank defines fraud and corruption as:

Fraudulent practice

A fraudulent practice is any act or omission, including a misrepresentation, that knowingly or recklessly misleads, or attempts to mislead, a party to obtain a financial or other benefit or to avoid an obligation.

Corrupt practice

A corrupt practice is the offering, giving, receiving or soliciting, directly or indirectly, of anything of value to influence improperly the actions of another party.

Top three areas for risk

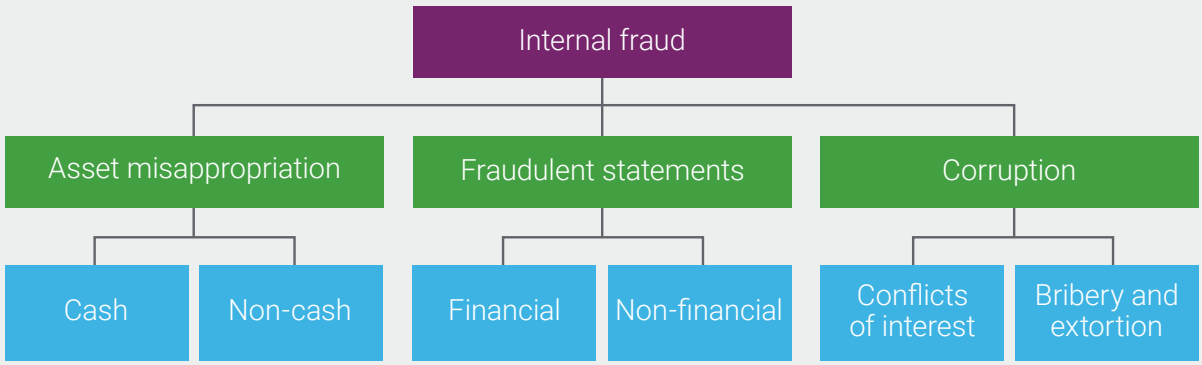
There are three main categories of fraud that affect organisations:

Asset misappropriation, which involves the theft or misuse of an organisation's assets. Examples include: theft of plant, inventory or cash, false invoicing, accounts receivable fraud and payroll fraud.

Fraudulent statements usually in the form of falsification of financial statements in order to obtain an improper benefit. It also includes falsifying documents such as employee credentials.

Corruption such as the use of bribes or acceptance of kickbacks, improper use of confidential information, conflicts of interest and collusive tendering.

Types of internal fraud



Source: Fraud Risk Management – A guide to good practice, CGMA, 2012

It is important to recognise that in addition to financial fraud, non-financial information may also contain fraudulent data, if information pertaining to the action described is falsified. These risks are particularly high in the supply chain and can cover a range of actions related to non-financial information, such as bribery in kind, concealing activities such as forced and child labour, environmental impact and inappropriate use of data, and falsifying records, statements and information about a product, service or the organisation itself.

All these areas intersect with business activities that a management accountant has input into or oversight of, so being alert to irregularities and questionable information is critical.

Risks to an organisation are rarely limited to factors under the direct control of the organisation. The wider value chain and all those that are engaged in the supply chain also represent the potential for fraud and corrupt practices to impact on the business and its stakeholders.

Examples of fraud and corruption

The SME and bribery

In the UK in 2014, a small limited company specialising in printing security documents, together with its chairman and its sales and marketing manager, were convicted of corruptly agreeing to make payments totalling nearly half a million pounds. These payments were used to influence the award of business contracts in Kenya and Mauritania. This was the first Serious Fraud Office (SFO) trial resulting in conviction of a corporate for foreign bribery.

Whistleblowing from the top

In 2011, Japanese giant Olympus became engulfed in a $1.7 billion accounting scandal after its former Chief Executive was dismissed for questioning company accounts and brought the issue to global attention. As a result of the scandal, the Board resigned and the company together with three former executives pleaded guilty in Japan to charges related to a cover-up. The scandal had a devastating impact on the value of the company at the time and the company was fined ¥700 million (£3.8 million).

Defrauding government

In South Africa in 2016, a businessman was sentenced for 20 years for using a multimillion South African rand fishing business as a front for false VAT returns, using the proceeds to fund an excessive luxury lifestyle and losing the country's revenue service over R250 million.

Endemic misreporting ends a company

Satyam Computer Services, an Indian global IT company, was brought down and joined the ranks of Enron and WorldCom on the scale of fraudulent financial activity, after the CEO in 2009 admitted the company had misrepresented its accounts to its board, the stock exchanges, the regulators, its investors and all other stakeholders. The company's revenues and profits were overstated, and it also reported a cash holding of approximately $1.04 billion that simply did not exist. The CEO, together with others involved in the fraud, were convicted in 2015.

It is widely recognised that in recent years there has been an increased focus on business ethics, driven in part by the many high-profile business scandals that have caught global attention. But beyond the front-page headlines of major corporate fraud or corruption cases from all corners of the world, such as FIFA, Petrobas or Toshiba in the last two years, there are countless more incidents of fraud and corruption impacting organisations of every size and every sector globally. No organisation, or finance professional, can be complacent about the risk of either wrongdoing taking place somewhere within the organisation, or being targeted by external fraudsters.

Ongoing high-profile scandals have affected the trust that the public hold in business and those who run business. Worryingly, with this comes a lack of trust in governments globally. The Organisation for Economic Co-operation and Development (OECD) report[i] that over half of citizens in developed countries distrust their government. Fraud and corruption were cited among the main factors to explain the prevailing distrust. Recent years have seen numerous examples of citizens taking to the streets globally to protest about such issues and calling to stem corruption in government and business. Earlier in 2017 there was reportage on ongoing protests in Romania and Russia, following actions in Kenya, Brazil and elsewhere in 2016.[ii]

For professional accountants, who have a duty to uphold integrity and objectivity, there is a clear requirement to not knowingly misrepresent facts or subordinate their judgment to others, and to be straightforward and honest in all professional and business relationships (see CGMA Code of Ethics). With their training in analysing and interpreting data, both financial and non-financial, they are in a position to challenge information that seems suspicious, and to be diligent in examining the supply chain, as well as interpreting where there most likely is high risk – be that in a market, product line or through partners and suppliers. By being alert to issues that undermine business integrity and trust and by promoting both their Code and the focus on stewardship within the Global Management Accounting Principles,[iii] CGMA designation holders are well placed to champion better business for the long term.

Case study

Volkswagen (VW) Diesel Fraud: Running on empty

In 2015, the United States' Environmental Protection Agency (EPA) found that many VW cars being sold in America had a "defeat device" – or software – in diesel engines that could detect when they were being tested, changing the performance accordingly to improve results. At the time, VW was positioning its diesel cars in the markets, backed by a huge marketing campaign, highlighting its cars low emissions. The resultant scandal impacted on VW globally at every level of the company.

In early 2017, several VW executives were charged over their alleged roles in the emissions scandal. The US Attorney General stated that "These individuals all held positions of significant responsibility at VW, including overseeing the company's engine development division and serving on the company's management board.

Over the course of a conspiracy that lasted for nearly a decade, they seriously abused those positions, and today, they are being charged with a range of crimes, including conspiracy to defraud the United States, violations of the Clean Air Act, and wire fraud."

Investigations into their conduct are ongoing and followed a requirement concluded in 2016 for VW to pay $4.3 billion in criminal and civil penalties and to take specific measures to prevent future violations. These sanctions are in addition to more than $15 billion in settlements with VW that have previously announced and do not take into account other worldwide actions, including civil class actions, against the company.[iv]

2 The fight against fraud and corruption

The fight against corrupt practices has included the strengthening of anti-bribery legislation and the enforcement of laws preventing bribery by nationals overseas. A number of countries worldwide have revised their regulation at a local level, and at supranational level the United Nations, European Union and African Union have been active.

Fighting fraud and corruption, including at a corporate level, has also been a recent focus for G7 and G20 meetings as bribery and corruption is recognised as an impediment to economic growth. The G20 has also highlighted the abuse of legal and corporate structures to hide or conceal criminal activity as a critical issue in the global fight against corruption. This was a theme also prioritised by the 2016 global anti-corruption summit held in London by the then Prime Minister as part of a unified drive to expose, punish and drive out those guilty of corruption. The summit resulted in the first-ever global declaration against corruption. Leaders had shared a common ambition to tackle corruption together with specific actions at country level. A total of 648 commitments were made by 43 countries.

The International Federation of Accountants (IFAC) recognise the crucial role professional accountants play, alongside other key actors in the economy, to tackle corruption globally. They identify three vital things that need to happen:

Collaborative efforts across all sectors – business, government and the professions – must be intensified to enact clear organisational governance standards and whistleblowing protections for those who suspect or identify wrongdoing

Given vast public sector spending global interest in robust transparent and accountable public financial management must be reinvigorated

To support the public interest, there must be greater public adoption of high-quality international standards on financial reporting auditing and ethics

The Accountancy Profession – playing a positive role in tackling corruption. February 2017

IFAC have recently introduced a new international ethics standard, **Responding to Non-Compliance with Laws and Regulations**.[v] It sets out a framework to guide professional accountants in what actions to take in the public interest when they become aware of a potential illegal act, known as non-compliance with laws or regulation, or NOCLAR, committed by a client or employer, including issues of fraud and bribery. Professional accounting bodies globally are currently reviewing how to incorporate NOCLAR into their Codes with additional guidance where appropriate.

Such actions increase the pressure on the public and private sectors, and their officers, to mitigate fraud and corruption risks. This is reflected by the strengthening of legislation and action, as well as increased calls for prosecutions of individual executives, and public officials, in addition to actions against companies for corporate misdemeanours.

Punitive costs cases

Corruption on a global scale

The largest Foreign Corrupt Practices Act fine to date of $800 million related to Siemens, a German-headquartered technology company. This was just a proportion of the overall estimated €2.5 billion in fines from several markets in relation to the global corruption scandal uncovered in 2006. Investigations were reported to cover business representing 60% of Siemens' revenues across operations in Asia, Africa, Europe, the Middle East and the Americas and resulted in a change of top management, global compliance structures and a step change in embedding a corporate culture.[vi]

Corruption on a local scale

Rita Crundwell – former treasurer and comptroller of the city of Dixon, Illinois – committed one of the largest municipal frauds in US history. She was sentenced to nearly 20 years of imprisonment after defrauding the city of $53.7 million. She orchestrated the fraud by redirecting money from various city accounts into a secret account that she had opened in the name of the city.

3 What are the costs of fraud and corruption?

Corrupt practices engender high cost: to the business or organisation itself, to the sector it operates in and to the wider economies, therefore impacting society at large. For those in the poorest countries the cost can be highest when fraud and corruption leads to failures in government services, governance and regulation and correlates with a loss of both livelihoods and lives. Estimates show that the cost of corruption equals more than 5% of global GDP ($2.6 trillion, World Economic Forum) with over $1 trillion paid in bribes each year (World Bank).

Impacting the global economy and market performance

At a global economic level the Organisation for Economic Cooperation and Development (OECD) finds that integrity can significantly boost inclusive growth and sustainable development, by:

- assuring fair and efficient resource allocation
- stimulating competition and investment
- and fostering innovation

The promotion of responsible business conduct is important in levelling the playing field for all companies in the market, and also creates an investment climate that is conducive to competition, innovation and business development. Bribery of public officials and other corrupt practices is a direct risk to this and can undermine equality and prosperity of societies by impacting negatively on revenue collection, public finance management, service delivery and thus the public interest. Corruption ultimately can exclude poor people from public services and perpetuates poverty. The significant impact of corruption on income inequality and the negative effect of corruption on income growth for the poorest 20% of a country have been proven empirically, by creating barriers for access to services, or even exclusion.[vii]

At a company level corrupt activities add additional costs to a transaction. It is estimated that each year a typical organisation can lose on average 5% of its annual revenue to fraudulent behaviour.[viii]

Corruption brings risks of prosecution, high financial and operational penalties, blacklisting and reputational damage (see the UNGC box). It also limits business certainty. If companies are paying bribes in order to win business, who's to say a competing company might not win, just by paying more? Buying decisions that are divorced from the best bid or project outcome can have further serious repercussions in the marketplace.

Why should companies care?

Principle 10 of the United Nations Global Compact (UNGC) relates to anti-corruption and calls on "business to work against corruption in all its forms, including extortion and bribery."

The UNGC recognise that the rapid development of corporate governance rules around the world is also prompting companies to focus on anti-corruption measures as part of their mechanisms to express corporate sustainability and to protect their reputations and the interests of their stakeholders. Their anti-corruption systems are increasingly being extended to a range of ethics and integrity issues, and a growing number of investment managers are looking to these systems as evidence that the companies undertake good and well-managed business practice.

Businesses face high ethical and business risks and potential costs when they fail to effectively combat corruption in all its forms. All companies, large and small, are vulnerable to corruption, and the potential for damage is considerable.

Businesses can face:

Legal risks: not only are most forms of corruption illegal where they occur, but it is also increasingly becoming illegal in a company's home country to engage in corrupt practices in another country

Reputational risks: companies whose policies and practices fail to meet high ethical standards, or that take a relaxed attitude toward compliance with laws, are exposed to serious reputational risks. Often it is enough to be accused of malpractice for a company's reputation to be damaged, even if a court subsequently determines the contrary

Financial costs: there is clear evidence that many countries lose close to $1 trillion due to fraud, corruption and shady business transactions, and in certain cases, corruption can cost a country up to 17% of its GDP, according to the UN Development Programme in 2014. This undermines business performance and diverts public resources from legitimate sustainable development

Erosion of internal trust and confidence as unethical behaviour damages staff loyalty to the company due to involvement in illegal activities etc.

Source: https://www.unglobalcompact.org/what-is-gc/mission/principles/principle-10

Corrupt practices: Zero return for high risk

A 2016 Harvard Business School study on bribery by Professors Serafeim and Healy shows that while corrupt practices may substantially boost local sales in the short term, in the longer term their overall effect on a company's finances are nil, and if such practices are exposed, additional costs, financial and non-financial, will be detrimental, thus making it a high-risk activity with potential for huge loss. The study's authors found that weaker corruption controls and enforcement can allow firms to generate higher sales growth in high-corruption markets. However, this is offset by costly bribes, and "the low returns on equity on incremental sales in high corruption markets for firms (that commit bribery) imply that the costs are not fully recovered through higher prices on corrupt contracts or through scale economies from increased sales." [ix]

The value of people

Previous work by Serafeim and Healy on firm competitiveness and detection of bribery has also shown additional longer-term intangible costs of bribery. They found it had a significant impact on corporate performance due to the negative effect on employee morale. As Serafeim concluded, "The lesson for managers is that bribery is more costly than you might think. If you think of the cost as just fines and regulatory actions, you're missing a big piece of the puzzle." In addition to low morale post-scandal, there will also be issues in relation to attracting talent.

Once corrupt activities are identified within an organisation this creates additional time and resource costs related to crisis management activities. Different levels of management, from the Board downwards, will need to be involved in both investigating and redressing the problem, with the need for buying in specialised assistance, ongoing interaction and cooperation with authorities, regulators as well as the press and consumers. The follow-up actions needed to address the issue, and any necessary restructuring to mitigate future issues, will also be resource heavy and may detract from other areas of the business and overall performance. Budgeting for fraud prevention, therefore, can be more economical than dealing with the repercussions of fraud.

The effect on reputation can sometimes have the most significant impact and can even bring a company down. When we asked CGMA designation holders in 2014[xi] what ultimately drives employers' motivation to embed ethical standards, the reputational view of stakeholders was the most frequently selected value driver. This reputational concern was seen as more important than issues of compliance, regulations and legislation. This points to a growing recognition of the tangible business benefits of an ethical culture. Reputation is what shapes an organisation's relationship with all stakeholders, and once it is undermined, so too is the business.

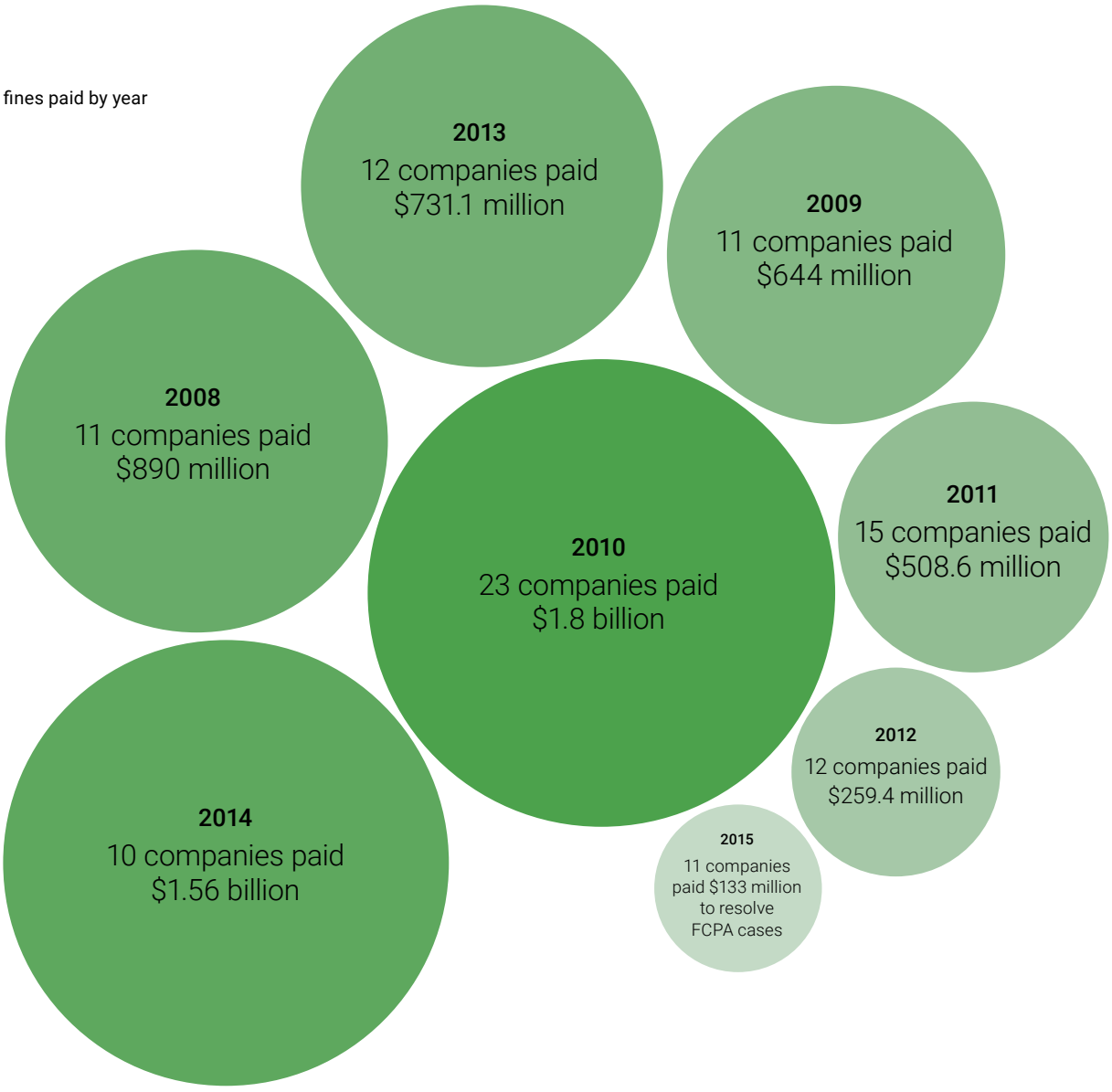
Regulatory and legislative actions

Organisations are of course required to comply with the law and regulations in the framing of their activities. Enlightened organisations may often go further than compliance in order to sustain responsible business, recognising that today's ethical trend may be tomorrow's law. In relation to anti-corruption there has been an increasing volume of legislative action in the last few years, and this momentum is set to build.

Regulatory fines: FCPA cases increase to record levels in 2016[xii]

The Foreign and Corrupt Practices Act (FCPA) enforcement index showed that in 2016, 27 companies paid about $2.48 billion to resolve FCPA cases. It was the biggest enforcement year in FCPA history. Both the number of enforcement actions and the overall amounts paid to resolve them were records. 2016 also saw a focus on cases against individual executives and foreign officials.

Total FCPA fines paid by year



Source: http://www.fcpablog.com

Rise in global bribery investigations

In regard to investigations, according to Trace International's Global Enforcement Report[xiii] , the US was also in the lead in pursuing cases. Enforcement actions since 2015 doubled (to 128) and represented 46% of cases globally.

However, non-US enforcement actions more than doubled in the same period. European countries remain at the forefront of this trend, together accounting for 42% of all open investigations. The UK remains the leader within Europe with 29 open investigations, followed by Germany with 17. Countries outside of the US have maintained their enforcement efforts against the acceptance of foreign bribes by domestic officials, with current investigations outstripping past enforcement actions by a factor of more than two. As was the case last year, Brazil leads the way with 22 open investigations, following by India (13), China (12) and Nigeria (10).

The engineering and construction industries, as well as the extractive, manufacturing and service industries, are under the most scrutiny. Transportation and communications are also represented highly in foreign enforcement.

Personal accountability stance

The EY Fraud Survey of 2016[xiv] found that 83% of respondents view enforcement against management as an effective deterrent against fraud, bribery and corruption. In the last few years influential markets have acted to strengthen personal accountability.

In the US in 2015, the Yates Memo,[xv] in the name of the then Deputy US Attorney General, stated: "One of the most effective ways to combat corporate misconduct is by seeking accountability from the individuals who perpetrated the wrongdoing." It provides guidance in the US for attorneys to bring cases against individuals for corporate wrongdoing. Its significance is in how it highlights an increased appetite in the US, and globally, for bringing individuals implicated in corporate crime to account.

The clawback policies were also introduced by the Securities and Exchange Commission (SEC) in the Sarbanes – Oxley Act of 2002 (SOX) so that companies can recoup incentive compensation that was paid to executives based on financial statements that were later found to be misstated.

The UK's Bribery Act 2010 also highlights penalties for individuals. If an individual is found guilty of a bribery offence, tried as a summary offence, they may be imprisoned for up to **12 months** and fined up to £5,000. Someone found guilty on indictment, however, faces up to **10 years' imprisonment** and an unlimited fine.[xvi]

Duty to prevent

The 2010 UK Bribery Act contains within it a powerful incentive to commercial organisations to prevent bribery by implementing procedures to promote an anti-corruption culture and mitigate wrongdoing, since such procedures provide a defence under the Act to the criminal offence of failure to prevent bribery. The UK is also poised to introduce a new corporate offence of failure to prevent the criminal facilitation of tax evasion, under the proposed Criminal Finances Act. Companies will be required to put in place reasonable prevention procedures to stop someone acting for or on their behalf from facilitating tax evasion whether in the UK or abroad. A company that fails to do so can be prosecuted and faces an unlimited fine. Both the legal and accounting professions are highlighted within the proposed Act.[xvii]

The UK may also consider introducing new corporate criminal liabilities arising from a failure to prevent economic crimes such as fraud, money laundering and false accounting, following a Call for Evidence on the reform of corporate criminal liability for economic crime issued by the UK government in January 2017. It is likely that any new legislation would reflect similar corporate offences under the Bribery Act (where a company will be guilty of a criminal offence where an associated person commits bribery, unless the company can prove that it had adequate procedures in place to prevent such conduct).

The relevance of both introduced and proposed legislation is the global impact. The last decade has seen a significant increase in governments and multilateral organisations working together in fighting corruption, with resultant national legislation that will have far-reaching effects. It also underlines trends that many local lawmakers will follow.

Professional accountants, guided by their Code and training, are well placed to be alert to corruption risks. They have an important role to play in influencing the organisation by having the right systems in place, contributing to the culture and escalating identified issues promptly for resolution, in order to safeguard the organisation. In this way they also help embed prevention processes within organisations.

See our accompanying anti-corruption briefing, Anti-Corruption Landscape 2017, which features the TI Global Corruption Perceptions Index (ranking corruption risk by market), as well as highlighting key aspects of FCPA, the UK Bribery Act and other corruption laws in selected markets.

4 Key actions in identifying and mitigating fraud and corruption risks

Despite the ever-present risks of corruption, CGMA research[xviii] in 2015 found that globally only 57% of organisations have specific **anti-corruption guidelines** – rising to 78% among the largest organisations. Given that in the same survey, 80% viewed bribery as an ethical issue of relevance to their organisation, it is imperative that a company's reporting and risk routes are stated more explicitly in relation to fraud and corruption threats.

The most critical aspect in safeguarding an organisation is the **overall culture and governance systems**. The overall ethos and the framework and architecture to support this, including formal roles and responsibilities, internal controls, codes of conduct and other related policies, should all emphasise a **zero tolerance** of any corrupt practices.

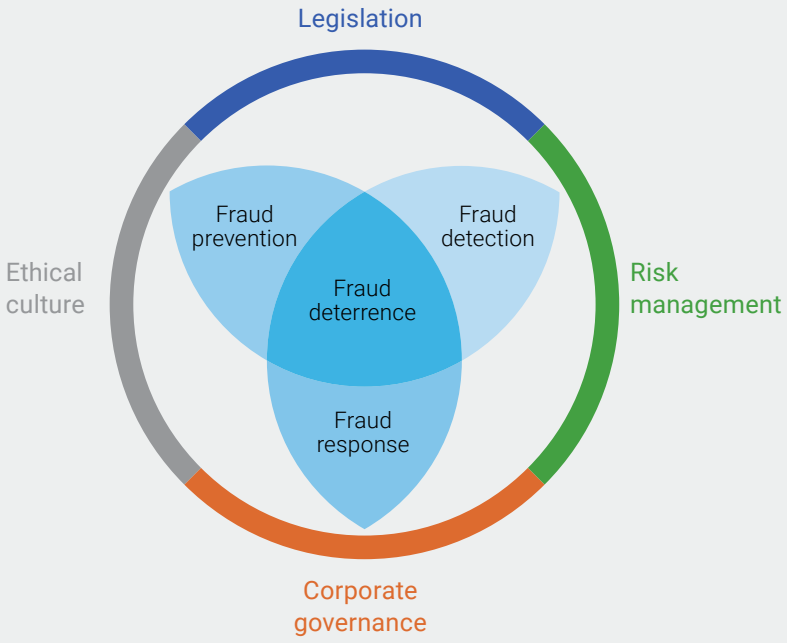
"Strong governance is crucial to trust and integrity in all sectors of the global economy. It is the foundation for recovery, growth, and stability, and is essential to the global fight against fraud and corruption. It enhances governments' decision making, supports disclosure of more valid information, and promotes more robust conduct and ethical behaviour."

IFAC: Trust and Integrity the Accountancy Profession's Call to Action by the G20.

An effective strategy in addressing fraud and corruption risks within the business is made up of four main components: **Prevention, Detection, Response, Deterrence** – and all aspects need constant communication and revisiting. Risks are ongoing and ever-changing, made more complex with advances in technology, and the number of relationships within the supply chain.

Anti-fraud strategy

The following diagram summarises these components and the context within which an anti-fraud strategy sits.



Fraud risk management: A guide to good practice, CGMA 2012

According to the COSO Fraud Risk Management Guide[xix], **deterrence** is achieved when an organisation implements a fraud risk management process that:

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture
- Includes a thorough fraud risk assessment periodically
- Designs, implements and maintains preventive and detective fraud control processes and procedures
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in wrongdoing

The frontline in fighting fraud and corruption lies with employees. They are closest to observing wrongdoing and your main source of deterrence and escalation. Those in finance particularly have an important role in assessing risk. Creating an environment that enables speaking up and clear routes to addressing areas of concerns, and for the organisation to be seen as taking action, are the first and most important lines of defence. Who you are hiring in is also critical for the culture. Ensure that you are applying ethical due diligence in both recruitment and promotion processes.

Internal controls and how they are managed and followed up on are critical. Having a clear process to follow up on any potential "red flags" – the indicators of potential issues regarding governance failure, collusion or corruption in the business or related ventures – helps mitigate problems early on. The presence of anti-fraud controls, such as management reviews and telephone hotlines, can greatly reduce the damage done by fraud schemes. Research has shown that fraud schemes executed at organisations that implement anti-fraud controls continue for significantly less time and inflict much smaller losses.[xx]

Collective action, through alliances with like-minded organisations, particularly in high-risk markets, can be an important step in countering corruption and enhancing transparency in business.

All those charged with oversight and governance need to be prepared when an incidence of fraud or corruption occurs, as there is an inevitability that there is ever-present risk.

Questions for those charged with oversight, from a financial manager to the Board, should include:

What is the top-level commitment to fighting fraud and corruption, and what resources do we have to support this?

How is our relationship with the regulators? How do we work together?

How can we identify the red flags in our wider supply chain or partner network? What due diligence is in place before entering contracts, and, managing risks on an ongoing basis?

How are anti-fraud and anti-corruption processes ingrained in our control processes? Are they proportionate to our risks, circumstances and culture?

What training and awareness raising is in place for all our staff related to fraud and corruption? How is this tiered in relation to their responsibilities and exposure?

How are our people equipped to manage sensitive negotiations and to escalate as necessary?

Are speak-up/whistleblowing lines in place, known about, trusted and used? Do staff feel supported and are they encouraged to use them?

What plans are in place to investigate wrongdoing when it arises, and are we consistent in our actions?

Are we transparent about how we tackle wrongdoing? Are those found culpable of wrongdoing dealt with appropriately?

How are we monitoring the implementation and effectiveness of our anti-corruption programmes, and how does this feed back into improvements?

Do we have a crisis management plan in place should the worst happen?

Do we know what to do if someone alerts me to a risk? What are the next steps we would take?

Deterrence is achieved when an organisation implements a fraud risk management process that:

- Establishes a visible and rigorous fraud governance process
- Creates a transparent and sound anti-fraud culture
- Includes a thorough fraud risk assessment periodically
- Designs, implements and maintains preventive and detective fraud control processes and procedures
- Takes swift action in response to allegations of fraud, including, where appropriate, actions against those involved in wrongdoing

The resources section of this briefing signposts to many sources to help guide you through addressing any of these issues that you have shortfalls with or need to understand better.

Eight ways to fight the fraudsters

Beyond the high-profile cases, most finance directors are most worried about the low-level fraud that affects their organisation. The following table features eight practical tips from experts to help organisations of all sizes address fraudulent practices:

1

Provide leadership from the top

"Setting an anti-fraud policy and leading by example improves attitudes towards fraudulent activities and sends out a message that it will not be tolerated," says Kellie Edwards, head of forensic practice at Salamanca Risk Management, a security and operational risk firm. "Board members need to be encouraged to speak to all related parties, including staff, customers and suppliers at all levels," she says.

2

Identify the key risks

Many organisations don't even consider fraud to be a key risk, argues Alex Plavsic, head of KPMG Forensic UK. "This is often a combination of the poor capture of fraud within an organisation – hidden in losses such as stock write-offs, claimant errors or budget over-runs, and a lack of awareness of the organisation's fraud risks and how they would manifest themselves. Properly capturing and reporting fraud often pushes it up the agenda at organisations. One practical way of identifying whether it's under-reported is to benchmark reported fraud against the experiences of comparable organisations."

3 Promote an anti-fraud culture

"A strong tone from the top lets employees know that the executives, the board and management have faith in, and rely on, the compliance program for ferreting out fraud and abuse," says Tracey Stretton, legal consultant and e-disclosure expert at Kroll Ontrack Legal Technologies. "A company must also invest time and resources in its staff," adds Mike Wright, partner at BTG Global Risk Partners. "Initiatives, such as employee share schemes and team performance rewards, can not only discourage internal fraud, but also encourage employees to identify external fraud."

4 Develop effective anti-fraud controls

"When organisations fall victim to supplier fraud it's often because when processes fail, there is insufficient awareness of the fraud among staff to make them query the payments," says Plavsic. "For example, the second signature needed to change the bank account details from the genuine supplier to the fraudster is just a tick-box exercise that doesn't include any scrutiny. Or the telephone confirmation is carried out using the phone number supplied by the fraudster, rather than the one held on file for the supplier."

5 Encourage and nurture whistle-blowers

David Lewis, convener of the International Whistleblowing Research Network, has the following tip for an effective whistleblowing policy: concerns should be raised through line management, but alternatives should be made available. As far as possible, people who ask for it should have their identity kept confidential and staff need access to free confidential advice. Screen allegations so that investigations are only conducted in appropriate cases. Feedback should be provided to disclosers in order to demonstrate that concerns are being taken seriously. All staff need training in the whistleblowing arrangements.

6 Develop a response plan

"The best time to plan is before a fraud occurs, not afterwards," says Will Kenyon, partner in PwC's forensics practice. "Be clear about your ultimate objectives, which may vary from one situation to another." Early steps need to secure evidence, reporting lines and PR strategy. Kenyon warns: "The occurrence of fraud may be out of your control, but the way you respond is within your control and you will be judged on it."

7 Harness technology to fight fraud

High-performance analytics is one of the biggest counter-fraud weapons since the advent of social network analysis, says Michael Rhodes, senior fraud consultant for SAS UK and Ireland. "The ability to analyze vast quantities of data in a relatively short space of time, or even real time, gives insight into customer or employee behaviors that may be indicative of fraud," says Rhodes.

8 Develop good internal controls

Aim to have 100 per cent of invoices linked to purchase orders, advises Adam Simon, global managing director of business development at PRGX, a business analytics and information services firm. "Moving from paperwork to electronic platforms makes it easier to monitor workflow and track invoices through the system," he says.

Companies can fight expenses fiddles – another common fraud – by adopting automated processes. "For example, linking the employee expense management system directly with the travel agent or flight booking system," says Gary Waylett, chief executive of Eclipse Group, which provides business management systems.

Source: Peter Bartram, Financial Management, CIMA, 23 August 2012

5 Spotlight on Executive Impersonation

Cyber-attacks are becoming the new normal to the point where it is no longer a question of 'if' but rather 'when' organisations will be victimised. These attacks have significantly grown in numbers over the past few years with more sophisticated and concealed schemes and greater financial impact and reputational damage to the victim organisation. Cyber-attacks are carried out through many methods and styles – from unauthorised web access, email phishing, password cracking and denial-of-service attacks to name a few – all with the objectives to steal valuable information and cause some level of harm and disruption to the targeted organisations.

Among the many forms of cyber-attacks, Business Email Compromise (BEC) is a new method that is attracting increased attention among senior leaders. According to the 2015 Internet Crime Report, "BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds."[xxi] Email Account Compromise (EAC) is another form of email scam but targets individuals instead of businesses.

BEC schemes target businesses of all sizes and across all geographies. These malicious hackers make no exceptions. Small companies are as exposed as large corporations are. The hackers will attempt to crack the most sophisticated and secured networks and capitalise on the slightest window of opportunity presented through poorly secured or vulnerable systems. Giant companies like Yahoo, eBay, Heartland and Netflix have not been exempted. The heist of the Central Bank of Bangladesh remains one of the biggest cyber-attacks in 2016. The hack resulted in $81 million in losses, and the money was reportedly transferred to the Philippines and other parts of Asia.[xxii]

The following BEC statistics were reported to the Internet Crime Complaint Center (IC3) from October 2013 to May 2016[xxiii] by victims in all 50 states and in 100 countries. The information is derived from multiple sources including international law enforcement agencies and financial institutions. According to the Federal Bureau of Investigation (FBI), there has been a 1,300% increase in identified exposed losses since January 2015. Other countries also have an equivalent internet crime complaint centre such as Action Fraud[xxiv] for the UK.

BEC statistics reported in victim complaints to the IC3 from October 2013 to May 2016:

Domestic and international victims:	15,668
Combined exposed dollar loss:	$1,053,849,635

Total **US** victims:	14,032	Total **non-US** victims	1,636
Total **US** exposed dollar loss:	$960,708,616	Total **non-US** exposed dollar loss	$93,141,019

Executive impersonation is an emerging form of BEC. It is a variation of the practice of spear phishing, where fraudulent emails are sent to select credulous employees – with certain privileges – in order to extract confidential information such as access codes, account numbers or other sensitive information. Executive impersonation allows criminal hackers to pretend to be a high-ranking executive and send a fake email to a mid-or lower-level employee urgently requesting to transfer large sums of money to known suppliers or between subsidiaries on behalf of the organisation. This usually takes place when the executive is travelling, usually out of the country, and cannot be reached in a prompt manner. The scheme is orchestrated by experienced hackers who have conducted extensive research on the targeted organisation. These researches include social media outlets, business reports, communications and other forms of company resources to understand the company's culture, operations, employees' behaviours and ethical principles. Such insight allows the hackers to carry out many hidden attacks – sometimes multiple times – on the same organisation.

The cultural mindset of the business landscape usually dictates a sense of urgency when an employee receives a request from a superior. This thinking is greatly emphasised when the nature of the request is from an executive and of a pressing matter with apparently valid and authentic documentation. Under these circumstances, the employee or accountant feels less inclined to question the request, go through all the required approval and control steps, and delay execution. The employee – in an attempt to act responsively to his/her superior – will drop everything to immediately wire the funds to the designated account. A few days usually go by before the employee follows up with the executive to discuss the transfer. By that time the funds have already disappeared from the fraudulent account and it is too late.

Below are **practice tips** to prepare organisations in the fight against cyber schemes. There are many ways that organisations can strengthen their structures and ultimately their weak spots. According to David Zweighaft, CPA, CFF, Managing Director of DSZ Forensic Accounting & Consulting Services, and member of the AICPA Fraud Task Force, "awareness, training and repetition are the best steps you can take to prevent Executive Impersonation fraud, but when this type of cyberattack is suspected, early mobilization and assessment of the impact are crucial."

Practice Tips

AICPA Forensic and Valuation Services Semi-Annual Report on Fraud Trends and Topics, Spring 2016

Train

Train employees responsible for wire transfers, placing a focus on BEC schemes and data security. Increase the frequency of training and provide updated information describing the latest schemes and trends in phishing and social engineering.

Establish procedures to verify the origin of all wire requests. Remind all employees to use the company fraud hotline to anonymously report suspicious activity without fear of retaliation.

Encourage a healthy level of skepticism in finance and treasury employees.

Engage

Engage cyber-risk security consultants to identify, monitor and mediate spear-phishing threats, including identifying employee-targeted attacks on social networks; finding and taking down fraudulent and impersonating accounts.

Continuously monitor key employee and company accounts for compromise.

Investigate attacks being planned against your organisation.

Review

Review policies and procedures for requesting, initiating and approving wire transfers.

Verify email requests by phone calls to company-registered phones.

Require two employees to approve wire requests and authenticate the recipient's identity before the wire is released.

Conduct

Conduct a risk assessment of the wire transfer process to identify weaknesses that could be exploited.

Engage a cybersecurity firm to perform a penetration test of the company's firewalls, email, security software, operating systems and browsers.

Flag incoming emails with domains that are similar, but not identical, to those of the company. Identify 'look-alike' domains and register them in the name of the company to prevent hackers from attempting BEC attacks.

Case study

Ubiquity Networks, Inc.

Ubiquity Networks, Inc. is an American technology company based in San Jose, California. The company manufactures and sells wireless data communication products. On June 15, 2015, the company was involved in a criminal fraud case and disclosed the attack in a quarterly financial report.[xxv]

According to the organisation, "the incident involved employee impersonation and fraudulent requests from an outside entity targeting the Company's finance department. This fraud resulted in transfers of funds aggregating $46.7 million held by a Company subsidiary incorporated in Hong Kong to other overseas accounts held by third parties. As soon as the Company became aware of this fraudulent activity it initiated contact with its Hong Kong subsidiary's bank and promptly initiated legal proceedings in various foreign jurisdictions.

As a result of these efforts, the Company has recovered $8.1 million of the amounts transferred. Furthermore, an additional $6.8 million of the amounts transferred are currently subject to legal injunction and reasonably expected to be recovered by the Company in due course. The Company is continuing to pursue the recovery of the remaining $31.8 million and is cooperating with US federal and numerous overseas law enforcement authorities who are actively pursuing a multi-agency criminal investigation."

After the attack and following proper investigation procedures, the organisation has strengthened its internal control over financial reporting procedures among others, as recommended by the investigation team.

In my role as Finance Director I am acutely aware of the constant cybercrime threats to our organisation and the increased priority placed on cyber security. As finance professionals we have a responsibility to minimise the risk. Firstly we must increase our awareness of the types of cybercrime that organisations face, and then be vigilant in all aspects of what we do and, applying our knowledge, actively work towards ensuring a cyber-breach does not occur.

Sarah Ghosh
BSc (Hons) FCMA CGMA, Finance Director, SweetTree Home Care Services Ltd, Member of CIMA UK Board and Chair of CIMA UK Network Panel

Cyber-attacks have become more widespread and damaging over the past few years. More than ever before, management accountants need to partner with business leaders within the organisation to be more vigilant on the rising trends of cyber threats. It is important for them to increase their understanding of these threats along with potential damaging impact on their organisations. Cyber-attacks affect not only the bottom line of an organisation but also its operations, brand, reputation and ability to innovate and attract customers. Management accountants – along with other business stakeholders – need to work together to constantly ensure the safety and security of the organisational networks and identify preventive, detective and restorable measures in case of any breach.

6 What's next? Further resources and information

The Association Resources

Code of Ethics and Professional Conduct
AICPA Code of Professional Conduct
CIMA Code of Ethics
CGMA Code of Ethics

For more information on implementation	Free	Paid
Do you really know who you are paying? (CGMA, 2017)	√	
COSO Fraud Risk Management Guide Executive Summary (COSO, 2016)	√	
COSO Fraud Risk Management Guide (COSO, 2016)		√
Ethical due diligence in hiring and assessing accountants CGMA, 2016	√	
Five steps to strengthen internal controls at small businessand not-for-profits (CGMA, 2016)	√	
Four critical reasons startups and smaller organizations need internal control (AICPA, 2016)	√	
Four strategies for curtailing internal fraud (CGMA, 2016)	√	
Four ways to ensure anti-corruption programmes are up-to-date (CGMA, 2016)	√	
Fraud hotlines: don't miss that call (Journal of Accountancy, 2013)	√	
Fraud Risk Management Guide (AICPA, 2016)		√
Risk management toolkit (CGMA, 2016)	√	
Risk culture in financial organisations (Joint report supported by CIMA, 2013)	√	
Risk and internal control: performance strategy (FM, 2013)	√	
Fraud risk management: A guide to good practice (CGMA, 2012)	√	

For more information on risk in supply chain	Free	Paid
4 steps to better manage global supply chain risks (CGMA, 2015)	√	
Ethics, risk and governance through the extended value chain (CGMA, 2014)	√	
Five ways to more effectively manage supply-chain risk (CGMA, 2014)	√	
How to make your supply chain hum (CGMA, 2014)	√	
Human rights risks in the supply chain (CGMA, 2016)	√	
Identifying fraud, waste, and abuse in the supply chain (CGMA, 2014)	√	
Modern slavery: Hidden risks to look for in your supply chain (CGMA, 2017)	√	
Seven key factors short-circuit supply-chain risks (CGMA, 2013)	√	

For more information on cyber risks and fraud	Free	Paid
AICPA Cybersecurity Resource Center	√	
Best practices to improve cybersecurity (CGMA, 2014)	√	
Executive impersonation: A growing threat (AICPA, 2016)	√	
5 steps CPAs can take to fight hackers (Journal of Accountancy, 2016)	√	
4 Cybersecurity Pitfalls to Avoid (AICPA, 2016)	√	
How CPAs can protect themselves and their clients (AICPA, 2017)	√	
IRM cyber risk report (IRM supported by CGMA, 2014)	√	
The top 5 cybercrimes (AICPA, 2013)	√	
Weak passwords only part of the cyber-security problem (CGMA, 2016)	√	
Web of deceit (FM, 2014)	√	

For more information on fighting fraud and corruption from global organisations

Organisation of Economic Cooperation and Development (OECD)	Provides a range of material in support of tackling bribery and corruption globally.
Partnering against Corruption Initiative (PACI)	Part of the World Economic Forum, PACI has become the leading business voice on anti-corruption and transparency. It leads regional and sectoral initiatives and is also focusing on implementing a global anti-corruption agenda with a focus on collective action.
UN Global Compact	Provides a range of practical tools, resources and information collated by global signatories in order to fight corruption.
Transparency International	It is an international movement that works with governments, businesses and citizens to stop abuse of power, bribery and secret deals. TI provides reports, guidance and updates at global, regional and country levels related to corruption. Its Corruption Perceptions Index is commonly used to assess risk at a country level by businesses worldwide.
World Bank anti-corruption	The Bank Group works at country, regional and global levels to build capable, transparent and accountable institutions and design and implement anticorruption programmes. It provides initiatives, guidance and resources to help tackle corrupt activities aimed at both public and private sectors.
International Federation of Accountants	IFAC provides guidance and information related to ethics, governance, risk and anti-corruption related to professional accountants globally.
Good Corporation	Provides information to tackle corruption, including a Framework on Bribery and Corruption. It sets out management practices that can be assessed to determine how well an organisation's safeguards work in reality.

Endnotes

[i] http://oecdinsights.org/2016/12/09/the-economy-of-influence-integrity-for-inclusive-growth/

[ii] https://www.theguardian.com/global-development-professionals-network/gallery/2016/mar/18/anti-corruption-protests-around-the-world-in-pictures

[iii] http://www.cgma.org/resources/reports/globalmanagementaccountingprinciples.html

[iv] https://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-delivers-remarks-press-conference-announcing-criminal

[v] https://www.ethicsboard.org/responding-non-compliance-laws-and-regulations

[vi] http://www.cgma.org/resources/reports/ethical-culture-change-at-siemens.html

[vii] http://oecdinsights.org/2016/12/09/the-economy-of-influence-integrity-for-inclusive-growth/

[viii] https://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

[ix] Crime Doesn't pay, says Harvard Bribery Study, CFO.com/ 032016 http://ww2.cfo.com/legal/2016/03/crime-doesnt-pay-says-harvard-bribery-study/

[x] Firm competitiveness Harvard Serafeim https://dash.harvard.edu/bitstream/handle/1/11508217/14-012%20(3).pdf?sequence=3

[xi] Ethical Performance, CGMA, 2014 http://www.cgma.org/resources/reports/ethical-performance.html

[xii] http://www.fcpablog.com/blog/2017/1/3/the-2016-fcpa-enforcement-index.html

[xiii] http://traceinternational.org/GER

[xiv] http://www.ey.com/gl/en/services/assurance/fraud-investigation---dispute-services/ey-global-fraud-survey-2016

[xv] Yates Memo https://www.justice.gov/dag/file/769036/download

[xvi] The UK Bribery Act http://www.legislation.gov.uk/ukpga/2010/23/contents

[xvii] Consultation on the corporate offence of failure to prevent the criminal facilitation of tax evasion http://www.legislation.gov.uk/ukpga/2010/23/contents

[xviii] Managing Responsible Business, CGMA, 2015 www.cgma.org/resources/reports/2015-managing-responsible-business.html

[xix] https://www.coso.org/Pages/Purchase-Guide.aspx

[xx] http://www.cgma.org/magazine/2016/mar/anti-fraud-controls-201614146.html

[xxi] https://pdf.ic3.gov/2015_IC3Report.pdf

[xxii] http://www.dailymail.co.uk/news/article-3599049/Hackers-81-MILLION-cyber-heist-one-world-s-biggest-Bangladesh-bank-NEVER-caught-untraceable.html

[xxiii] https://www.ic3.gov/media/2016/160614.aspx

[xxiv] http://www.actionfraud.police.uk/

[xxv] https://www.sec.gov/Archives/edgar/data/1511737/000157104915006288/t1501817_8k.htm

Interactive overview

Fraud and corruption in the global landscape

» Types of internal fraud

» Examples of fraud and corruption

» Case study: VW Diesel Fraud

Fighting against fraud and corruption

» IFAC's three ways to tackle fraud

» Punitive cost cases

Cost of fraud and corruption

» Principle 10 UNGC

» Serafeim and Healy, 2016 Harvard study

» FCPA enforcement index

» UK Bribery Act

Identifying and mitigating fraud and corruption risks

» Anti-fraud strategy

» Eight ways to fight fraudsters

Executive impersonation

» Business Email Compromise (BEC) statistics

» Practice tips: Train, Engage, Review, Conduct

» Case Study: Ubiquity Networks, Inc

Further Resources

» Association resources

» Implementation

» Cyber risk and fraud

» Fraud and corruption from global organisations

June 2017
ISBN no: 978-1-85971-844-5

aicpa.org

aicpa-cima.com

cgma.org

cimaglobal.com