Update: the exposure of small UK project management organisations to fraud [1]

Dr. Robert Chapman

Introduction

The purpose of this updated paper is to keep the subject of fraud on the 'radar' of project management organisations. Since writing the first article in May this year, the fraud landscape has changed significantly. The most important development is that fraud is on the rise and will likely increase even further due to changes to the UK economy. The predictions made by KPMG[2] are likely to prove accurate. The audit and assurance consultancy considers that widespread concern over the significantly increased costs of living in the UK, (driven by very substantial increases in food, fuel and energy costs), will be an added driver for insider fraud cases. Early signs are there will be a substantial rise in fraud committed by employees and management. In parallel, fraud committed by external 'actors' (criminals) is also on the rise. While PwC's survey[3] of 1,296 business executives across 53 countries and regions confirmed fraud remains ubiquitous, (with 46% of responding organisations reporting they had experienced fraud, corruption or another economic crime), of particular note is that the survey found a rising threat from external perpetrators "who are quickly growing in strength and effectiveness".

Cybercrime clearly poses the greatest threat. Perpetrators goals continue to be multi-faceted. Ken McCallum, of the UK's intelligence service MI5, has warned that fake profiles are being created on social networking sites such as LinkedIn and Facebook on an "industrial scale" with the view to building relationships with employees of high-tech businesses and others to ultimately securing sensitive information[4]. Similarly, vigilance is key, particularly when trading with new entities. Within the UK, a BBC investigation[5] uncovered that criminal gangs had set up over 100,000 fictitious companies at Companies House using the addresses of unsuspecting property owners. These owners have then had to deal with overdrafts, loans, insurance demands and credit card debts. The BBC's findings support the Treasury Committee Report referred to below under 'UK Government Initiatives'. On a more positive note, as announced by Brian Fung

[1] How to cite this paper: Chapman, R. J. (2022). Update: the exposure of small UK project management organisations to fraud; *PM World Journal*, Vol. XI, Issue IX, September.
[2] KPMG (2022) "Fraud Barometer: Annual Report for 2021, The latest fraud trends and patterns affecting the UK economy" and internet page, https://home.kpmg/uk/en/home/insights/2022/01/fraud-barometer.html
[3] PwC (2022) "PwC's Global Economic Crime and Fraud Survey 2022, Protecting the perimeter: The rise of external fraud". 61% of respondents occupied roles in the C-Suite.
[4] Sky News (2022) "Foreign spies using LinkedIn on 'industrial scale' to dupe government officials", Tuesday 17 May 2022, UK
[5] BBC (2022) "Bogus companies scam: We never knew our home was on the list" Shari Vahl, 11 August

of CNN Business[6], more than a dozen companies are collaborating on a single open standard for sharing data about hacking threats which it is hoped will help organisations detect cyberattacks more quickly. Those involved in developing the standard include Amazon, IBM, Salesforce, Cloudflare and CrowdStrike.

Research

The initial paper was based on research carried for the recently published book: "The SME business guide to fraud risk management" which found that "fraud is omnipresent and highly corrosive". Given the rise in fraud, the guidance contained in the book has gained greater importance. The previous paper aimed to provide: an insight into how toxic fraud is for small and medium sized enterprises (SMEs) together with a high-level overview of the degree of exposure to fraud; the types of fraud that may be perpetrated; a simple way of understanding their nature; and a possible response process. It also sought to provide an element of the context in terms of the scale of fraud and the government's response to what is a complex and evolving crime. The book highlights that SME's exposure to fraud can result in a loss of: clients; business partners; customer base; reputation; funds; and or staff. In addition, "a serious fraud event can result in a business struggling to recover for years, or even lead to its collapse"[7]. Fraud is estimated to be the most prolific crime in England and Wales[8]. Of significance is that it surfaces in a myriad of business functions and its perpetrators are constantly evolving new ways to search out company vulnerabilities. The most common types of fraud impacting project management organisations are procurement fraud, bribery, ransomware attacks, intellectual property theft, identity fraud, asset misappropriation fraud, financial statement fraud and business email compromise (including invoice fraud).

Incidence of fraud

According to the National Crime Agency (NCA), in 2019 fraud was the most common type of crime in England and Wales[9]. The NCA reported that there were an estimated 3.8 million incidents of fraud in the year ending September 2019, a third of all estimated crime, and an increase of 9% on the previous year. The trend continues. The Crime Survey for England and Wales estimated that in the year ending March 2020 there were 3.7 million incidents of fraud[10]. Fraud made up over a third (36 percent) of the total estimated crime and was the largest stand-alone crime type. The methods adopted by criminals to implement fraud are constantly evolving.

---

[6] Brian Fung (2022) "More than a dozen companies developing single standard to detect cyberattacks faster" CNN Business, 10 August 2022.

[7] Robert James Chapman (2022) "The SME business guide to fraud risk management", Published by Routledge in the UK and USA

[8] HMICFRS (2021). "State of Policing-The Annual Assessment of Policing in England and Wales". Her Majesty's Chief Inspector of Constabulary

[9] NCA (2020) The National Crime Agency's National Strategic Assessment of Serious and Organised Crime

[10] HMICFRS (2021) ''Spotlight report. A review of Fraud: Time to Choose, A revisit of the 2018 fraud inspection to assess progress of the recommendations and areas for improvement" https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/a-review-of-fraud-time-to-choose.pdf. Her Majesty's Inspectorate of Constabulary and Fire & Rescue Services (HMICFRS) .

UK Finance[11] have reported that they have seen the emergence of criminals openly advertising fraud and scam services for sale online, including template phishing websites and custom-built scam applications which replicate real banking applications.

Attention to fraud

Directors' meetings typically focus on health and safety processes, securing new business, new and existing commissions, changes in staff, invoicing, income and running costs. Topics of discussion may also include the more difficult subjects of staff disciplinary issues, client complaints, falling income, unpaid invoices, the imminent expiry of loan agreements or professional indemnity claims. Unfortunately, fraud risk management is rarely on a director's radar and is seldom included on director meeting agendas. This can prove to be ruinous. Particularly when it is assumed that fraud will only be perpetrated by those outside the organisation and not by employees. If you are the owner of and run a small project management organisation which you are seeking to grow, conversations you do not want to have with a client are you have been hacked and project information has been deleted, corrupted or stolen, or that you have had to let the project manager dealing with their project go, as the business has had to downsize as a member of the finance team had been stealing from the business, or yes the reports in the press that a member of staff has been found guilty of attempting to bribe a government official to win new business were true.

The cost of fraud to businesses

As identified in CIMA's and the CGMA's fraud risk management guides[12], surveys are regularly carried out in an attempt to estimate the true scale and cost of fraud to UK businesses. These and subsequent guides highlight that survey findings vary and it is difficult to obtain a precise picture as to the full extent of the country's exposure to fraud. However, these guides all paint a consistent picture; that fraud is ubiquitous and remains a very serious and costly problem. The cost of business disruption, including diminished employee productivity and business process failures (which occur after a cyberattack), continues to rise at a steady rate. According to the National Fraud Intelligence Bureau (NFIB), reported losses in the UK increased by 38% in the financial year 2018/2019, to £2.2 billion. This may have been a very conservative figure. The Santander Bank has reported that total fraud losses to UK SMEs were estimated to be £19bn last year[13].

Client expectations

Project sponsors, whether private clients or government departments, expect their consultants to have strong anti-fraud policies and training programmes which address protection against

[11] UK Finance is a professional body representing banking and finance industry organisations whose goal is to promote a safe, transparent and innovative banking and finance industry.

[12] CIMA (2008), "Fraud risk management, a good practice guide", and CGMA (2016) the Chartered Global Management Accountant's report "Fraud risk management, a guide to good practice".

[13] Santander Bank (2022) "Fraud prevention", https://www.santandercb.co.uk/support/fraud-prevention

cybercrime as well as the actions of company insiders. These policies are also expected to address the employees of organisations engaged directly by the consultancy to deliver their services, such as sub-consultants, suppliers or joint venture partners. Increasingly sponsors are concerned about protection against the loss of intellectual property, the theft, corruption or release of project data, the sharing the details of personnel, (particularly where employees have gone through security screening-providing a copy of their passport, driving license and national insurance number), and building access information.

Exposure of fraud

There are a number of types of fraud to which project management organisations are exposed to as illustrated in **Figure 1** and briefly explained below.

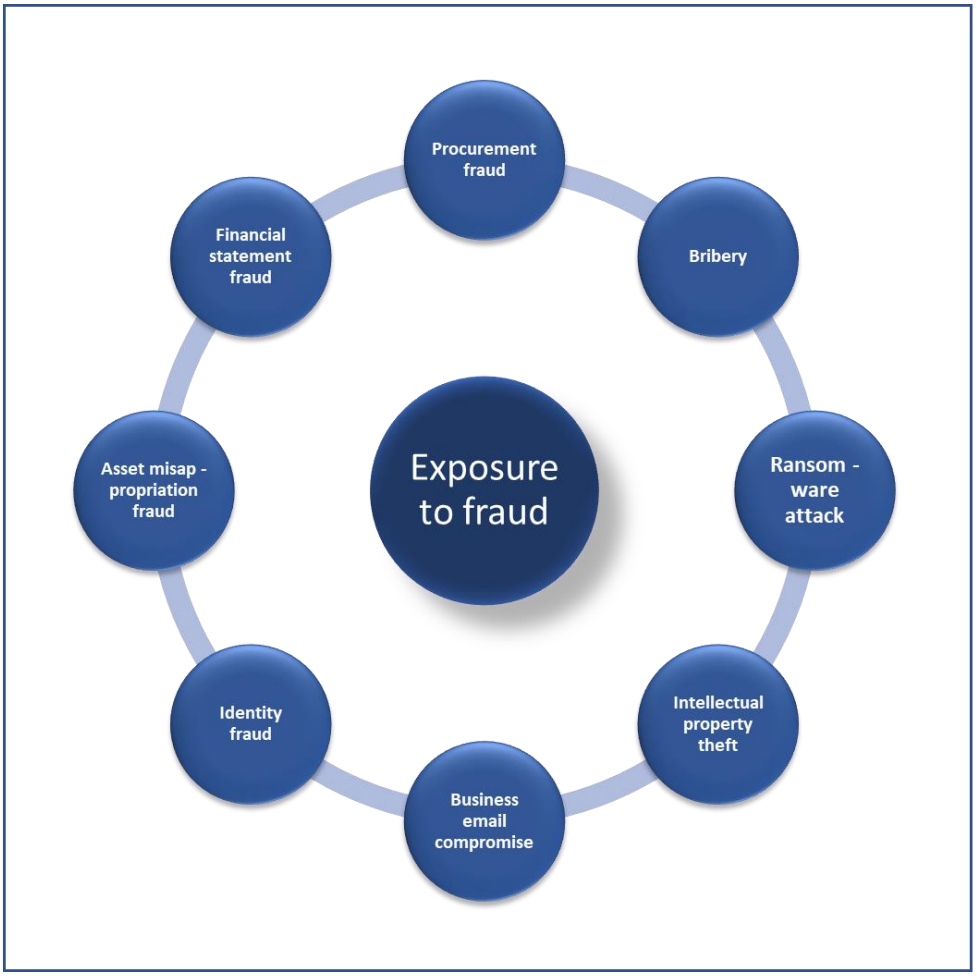


Figure 1: Project management organisations' exposure to fraud

Procurement fraud: refers to all unlawful activity that occurs throughout the sourcing, letting and management of contracts. It is recognised to be a complex problem given the different ways it may be perpetrated and the lengths offenders go to, to conceal their activity. In essence it is the unlawful practice related to the purchase of goods or services. A lack of awareness, understanding and detection creates an environment where procurement fraud can flourish.

Bribery: Fraud, bribery and corruption are often mentioned in the same breath. While they may be prosecuted under different legislation, these types of criminal activities have the same results in terms of tarnishing reputations or in some cases bringing about business closure-apart from possible custodial sentences and fines. For instance on 30 July 2020, the Serious Fraud Office announced it had brought charges against GPT Special Project Management Ltd and three individuals. On 28 April 2021, GPT pleaded guilty to corruption between December 2008 and July 2010 in relation to contracts awarded to GPT in respect of work carried out for the Saudi Arabian National Guard[14]. In sentencing GPT, the judge ordered the company to pay a confiscation order of £20,603,000, a fine of £7,521,920, and costs of £2,200,000.

Ransomware attack: Ransomware is a form of malicious software that enables cyber criminals to remotely lock down, steal, delete or encrypt files on a business's device. Criminals use ransomware to extort money from companies (a ransom) and will promise to restore access to a company's files or device once it has paid the ransom. The UK's Federation of Small Businesses (abbreviated to FSB) found that collectively businesses had been subject to 260,000 ransomware attacks over the previous two years[15]. There is no guarantee that once a ransom has been paid, access to data will be restored.

Intellectual property theft: Intellectual Property (IP) is often described as the lifeblood of many organisations. The significance of IP is described within a recent government report entitled 'Innovation increases productivity, grows markets an creates jobs'[16]. The types of IP most likely to be stolen by organised cyber criminals, state-sponsored and rival company hackers are initial concepts, designs and specifications. In the fight against the theft of IP, the Centre for the Protection of National Infrastructure's (CPNI), as part of its 'Think Before You Link' campaign[17], has developed an app "allowing users of professional networking sites to better identify the hallmarks of fake profiles used by foreign spies and other malicious actors". It has been developed with behavioural scientists to help individuals identify potentially fake profiles and report anything they believe to be suspicious. It has been reported that in the first half of 2021 alone, LinkedIn stopped 11.6m fake accounts at registration.

Business email compromise: Invoice fraud occurs when fraudsters divert genuine invoices or payment instructions sent by email, often from a familiar supplier or contact, and send a replacement email with the bank details changed to an account controlled by them. As reported by inews.co.uk[18], Barclays Bank has warned small and medium sized businesses that invoice fraud in particular is on the rise, which has resulted on occasion in businesses losing significant

[14] SFO (2021) "GPT Special Project Management Ltd". https://www.sfo.gov.uk/cases/gpt-special-project-management-ltd/
[15] FSB (2019) 'Small firms suffer close to 10,000 cyber-attacks daily' https://www.fsb.org.uk/resources-page/small-firms-suffer-close-to-10-000-cyber-attacks-daily.html
[16] Gov.uk (2022) "New app to counter malicious approaches online" https://www.gov.uk/government/news/new-app-to-counter-malicious-approaches-online. Published 17 May.
[17] https://www.gov.uk/government/news/new-app-to-counter-malicious-approaches-online
[18] inews Samantha Downes (2022) "Invoice fraud on the rise with average firm losing £2,100 as small businesses battle increasing costs", April 6. https://inews.co.uk/inews-lifestyle/money/small-business/invoice-fraud-on-the-rise-as-small-businesses-battle-increasing-costs-1559095?fr=operanews

sums. The bank has highlighted that this type of fraud accounts for 55 per cent of all money lost to fraud. Again, citing research by Barclays Bank, in 2018 Law firm Aberdein Considine reported that almost half of SMEs surveyed had been targeted by fraudsters, with nearly one in four of those targeted having fallen victim and as a consequence an estimated 50,000 jobs had been lost by SMEs due to diminishing order books.

Identity theft fraud: Identity fraud (often abbreviated to ID fraud) is also known as 'corporate identity theft', 'company hijack fraud' and 'corporate impersonation fraud'. Identity fraud can be described as the use of a stolen identity, obtained by criminal elements, to obtain goods or services by deception[19]. The UK government has warned businesses to be wary of identity fraud: "organised criminals attempt to steal the identity of honest businesses so that they can commit credit card and online banking fraud"[20] . The Companies House guidance 'How to protect your company from fraud and scams' offers 3 main ways to protect your company: register to file online, take appropriate security precautions and report any suspected fraud.

Asset misappropriation fraud: This type of fraud is explained in BOX 1 below**.** In a very recent case**,** not specific to a project management firm, a former financial controller at Clayton Technologies admitted one count of fraud by abuse of position and was sentenced on 20 April 2022 to three years in prison. The prosecutor said there were 246 suspicious payments into 10 different bank accounts totalling £362,103.73. The controller abused her position of trust to create false invoices and fictitious suppliers and used the money to buy a house, a car and overseas holidays.

BOX 1: Asset Misappropriation Fraud

As described by Action Fraud, asset misappropriation fraud involves third parties or employees in a business who abuse their position to steal from it through fraudulent activity for personal gain. It is also referred to as insider fraud. This type of fraud can be committed by company directors or its employees, or anyone else entrusted to hold and manage the assets and interests of a business. Typically, the assets stolen are cash or cash equivalents (such as credit notes or vouchers). However, the fraud can extend to include company data or intellectual property. At one end of the scale, asset misappropriation fraud may be limited to isolated cases of fraudulent expense claims or an employee lying about his or her qualifications to get a job. At the other end, it might involve organised crime groups infiltrating businesses to take advantage of weak systems and processes or inadequate internal controls. The definition of asset misappropriation fraud doesn't include straight theft from an organisation by insiders, such as stealing physical assets. Ultimately, it's the cash flow of the business that suffers. Action Fraud highlights that if they are not tackled, opportunistic one-off frauds can become systemic and spread throughout a business, creating a culture of theft and fraud. When this happens, fraudsters think their actions are the norm and as such acceptable. They have no moral compass and fail to make the distinction between company funds and their own

[19] Action Fraud. 'Identity fraud and identity theft'. https://www.actionfraud.police.uk/a-z-of-fraud/identity-fraud-and-identity-theft
[20] https://www.gov.uk/guidance/crime-and-fraud-prevention-for-businesses-in-international-trade

finances. At one end of the spectrum asset misappropriation fraud can erode an organisation's staff morale and reputation and at the other end cause job losses or even business closure.

Source: Chapman, R. J. (2022) "The SME business guide to fraud risk management", published by Routledge, UK and USA, April.

Financial statement fraud: Financial statement fraud is the deliberate material alteration of a company's financial statements in order to mislead and deceive the users of financial information to create either a healthier or more fragile picture of the company's financial position than actually exits. It involves the intentional overstatement and or the understatement of balances in the financial statements. The motivation for this type of fraud is to present a rosy picture when seeking to secure a bank loan, stakeholder investment or join joint venture bids for new contracts. Conversely financial statements may be manipulated to mislead HMRC on the level of profits achieved to reduce tax payments. The alteration of financial statements may be carried out by employees without the business owner's knowledge for personal benefit such as job retention, bonus payments, shares or a salary increase.

UK Government Initiatives

UK government reports on how to deal with fraud extend back decades. It is clear the methods adopted by criminals to perpetrate fraud is a moving picture. While email and internet banking have been adopted by businesses for many years now, their emergence has created a complex international dimension making fraud prevention more difficult. While the government, its agencies and police forces are striving to tackle fraud, collectively they are failing. A striking statistic is that in the year ending March 2020, less than 1 percent of all police personnel in England and Wales were involved in the investigation of fraud[21]. An indicator of the degree of success in responding to fraud is illustrated by an extract from the UK government's Treasury Committee Report on economic crime[22] included below. In summary, it considers the response of law enforcement agencies to fraud and allied crimes to be unfocussed, underfunded, uncoordinated and missing opportunities to reduce fraud. Economic crime is a broad term which the UK government defines within its 'Economic Crime Factsheet'[23] as relating to fraud, bribery, corruption and money laundering.

> *Economic crime seems not to be a priority for law enforcement. The number of agencies responsible for fighting economic crime and fraud is bewildering. Each of the enforcement agencies has other crime-fighting or regulatory objectives, and the Government needs to consider whether*

[21] HMICFRS (2021). "State of Policing-The Annual Assessment of Policing in England and Wales". Her Majesty's Chief Inspector of Constabulary [and] Police Workforce, England and Wales: 31 March 2020: data tables third edition, Home Office, 2020

[22] House of Commons Treasury Committee report 'Economic Crime', Eleventh Report of Session 2021–22 Published on 2 February 2022. https://committees.parliament.uk/committee/158/treasury-committee/news/160700/treasury-committee-publishes-report-on-fraud-scams-and-economic-crime/

[23] Home Office in the Media. 11 December 2017, https://homeofficemedia.blog.gov.uk/2017/12/11/economic-crime-factsheet/

> *there should be a single law enforcement agency with clear responsibilities and objectives to fight economic crime. The Government must ensure that law enforcement agencies are appropriately resourced to tackle the scale of the problem.*

A particular vulnerability highlighted by the Treasury Committee Report is Companies House[24]. The Report makes clear the necessity for modernisation which should be implemented expeditiously.

> *Reform of Companies House is essential if UK companies are no longer to be used to launder money and conduct economic crime. We welcome the work being done by the Department for Business, Energy and Industrial Strategy and by Companies House to modernise the legal framework and operations of Companies House. However, the pace of change is slow. The problems with UK company structures were identified by the Government in 2014.*

The Report also makes clear recommendations on specific reforms to be implemented. However there appears to be little appetite to make the changes required.

> *The low costs of company formation, and of other Companies House fees (such as filing fees), present little barrier to those who wish to set up large numbers of companies for dubious purposes. The Government should significantly increase the costs of Company and Limited Liability Partnership incorporation (including Scottish Limited Partnerships) and should review other Companies House fees to bring them closer to international standards. A fee of £100 for company formation would not deter genuine entrepreneurs, and would raise significant additional funding for Companies House and for the fight against economic crime.*

As identified by HMICFRS the intelligence database currently used by the National Fraud Intelligence Bureau (NFIB) known as the Strategic Analysis and Intelligence Platform (SAIP) commissioned to collect and analyse intelligence about fraud, is not fit for purpose. Since going live in October 2018 it has not operated as expected and it is understood that it not feasible to improve it. The intention is to replace it with a new database; however, this will not occur until 2024.

Comprehension of fraud

The pattern, mechanics, case studies and red flags for individual risks (see **Figure 2**) need to be understood to gain an appreciation of the vulnerabilities of a business to incidents of fraud. A

[24] Companies House is an executive agency, sponsored by the UK government's Department for Business, Energy & Industrial Strategy. Its role is to incorporate and dissolve limited companies. It registers company information and makes it available to the public.

brief explanation of these elements is provided below and a fuller description is provided in the book referred to in **Appendix 1**.

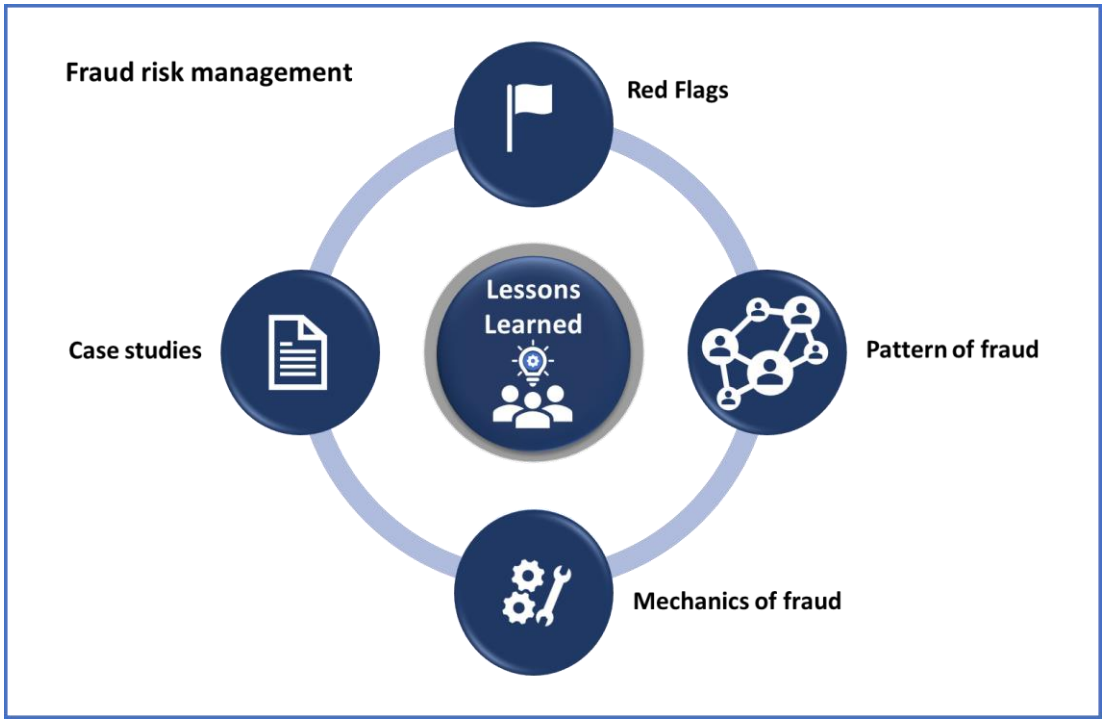


Figure 2: Fraud risk management (based on "The SME business guide to fraud risk management")

Pattern:	Describes the steps in a fraud attack or event.
Mechanics:	Describe the tools used by criminals to implement a fraud attack.
Case Studies:	Provide a historical record of fraud events and in particular provide information on aspects such as method, mechanics, scale of financial impact, perpetrators, changes in modus operandi, malware used, resilience (or otherwise) of backed-up data, exfiltrated data and resolution.
Red Flags:	Events that should they materialise, should alert employees, managers or directors to a fraud attempt.

Approach to fraud risk management

As described in "The SME business guide to fraud risk management" a possible approach to fraud risk management is the seven-step process illustrated in **Figure 3** below. It promotes a proactive approach to fraud management rather than a reactive one with the view to minimising exposure to fraud. It cannot eradicate the incidence of fraud altogether. The book describes each of the steps sequentially and assumes that businesses will be continuously learning and enhancing their risk management practices over time - as their knowledge matures and the fraud environment evolves. It should be stressed that as with all risk management practices, assessment of risk exposure together with response planning and implementation needs to be updated on a regular cycle.

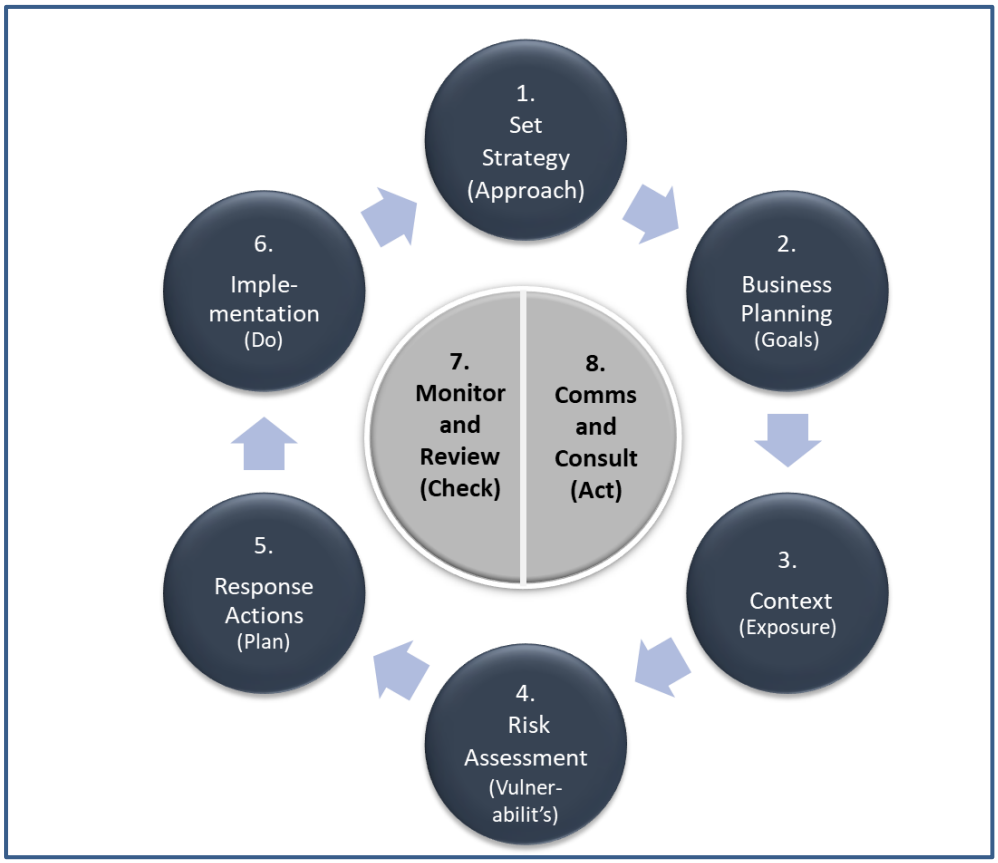
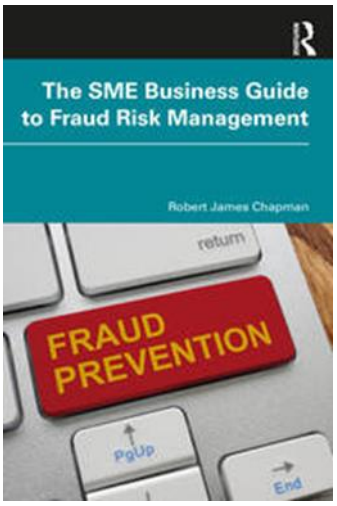


Figure 3: Approach to fraud risk management. (Based on "The SME business guide to fraud risk management" and reproduced with the permission of Routledge)

Summary

CEOs, Managing Directors and business owners of SMEs while having a multiplicity of pressures on their time must stay vigilant and be fraud aware. Cybercrime in particular is on the rise. Criminals are developing ways to attack tens of thousands of people with sophisticated software tools. As highlighted in numerous recent reports, given the prevalence of fraud and its damaging effects, it continues to warrant specific attention. It is inescapable. It is the most common form of crime in England and Wales. As an absolute minimum, businesses need to understand the forms of fraud, how they are perpetrated, the essential defensive measures that need to be put in place and the training that needs to be provided to employees. Tackling fraud is not an activity to put to one side to be addressed 'when there is time'. There needs to be an incremental roll-out plan. Plus, businesses need to be unequivocal when voicing to employees their zero tolerance to fraud in all its forms and be explicit when stating the discovery of fraud will lead to direct and swift consequences. Advice on tackling fraud is readily available. See Appendix 1 below which describes the recent publication "The SME business guide to fraud risk management".

Appendix 1: The SME business guide to fraud risk management



Publisher: Routledge; 1st edition (27 April 2022)

Language: English

ISBN 9781032055466

Author: Robert James Chapman

Formats: Paperback (and also Hardback)

Available from: Amazon

Currently available from numerous booksellers in England, America, France and Germany

Book Description

All organisations are affected by fraud, but disproportionately so for SMEs, given their size and vulnerability. Some small businesses that have failed to manage business fraud effectively have not only suffered financially but also have not survived. This book provides a guide for SMEs to understand the current sources of business fraud and the specific risk response actions that can be taken to limit exposure, through the structured discipline of enterprise risk management.

The book provides:

- A single-source reference: a description of all of the common fraud types that SMEs are currently facing - in one location.
- An overview of enterprise risk management: a tool to tackle fraud, as recommended by the Metropolitan Police Service and many other government-sponsored organisations.
- Illustrations of fraud events: figures (where appropriate) of how frauds are carried out.
- Case studies: brief case studies of the fraud types described, (to bring the subject to life and illustrate fraud events and their perpetrators), enabling readers to be more knowledgeable about the threats.
- Sources of support and information: a description of the relationship between the government agencies and departments.
- What to do: 'specific actions' to be implemented as opposed to just recommending the preparation of policies and processes that may just gather dust on a shelf.

The book gives SMEs a much better understanding of the risks they face and hence informs any discussion about the fraud prevention services required, what should be addressed first, in what order should remaining needs be addressed and what will give the best value for money.

About the Author

Robert J. Chapman, PhD, MSc.

United Kingdom

Dr Robert J Chapman is an international risk management specialist. He has provided risk management services in the UK, the Republic of Ireland, Holland, UAE, South Africa, Malaysia and Qatar on multi-billion programmes and projects across 14 different industries. He is author of the texts: 'Simple tools and techniques for enterprise risk management' 2nd edition, published by John Wiley and Sons Limited, 'The Rules of Project Risk Management, implementation guidelines for major projects' 2nd edition published by Gower Publishing and 'Retaining design team members, a risk management approach' published by RIBA Enterprises. He holds a PhD in risk management from Reading University and has been elected a fellow of the IRM, APM and ICM and is a former member of the RIBA. Robert has passed the M_o_R, APM and PMI risk examinations. In addition he has provided project and risk management training in Scotland, England, Singapore and Malaysia. Robert is an external PhD examiner.