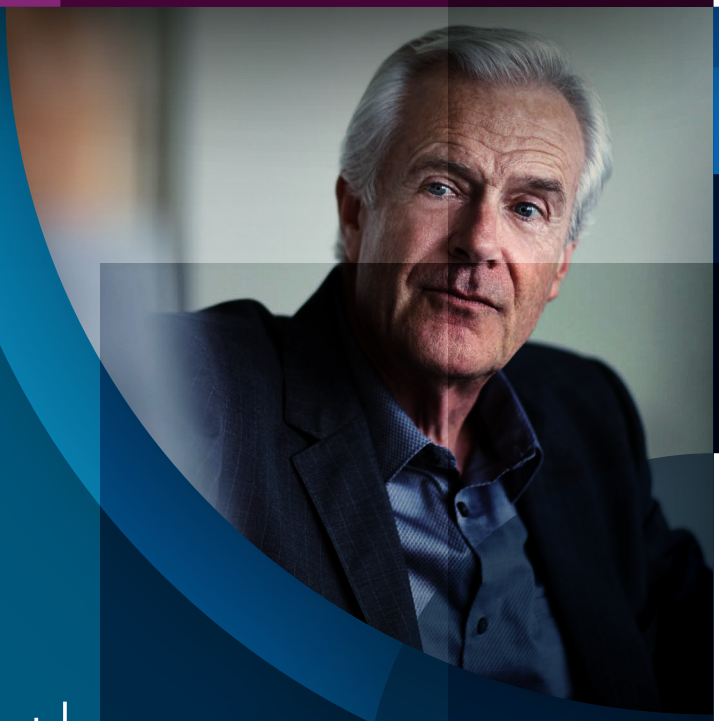


sas

Unmasking the Enemy Within

How smart analytics can stop procurement fraud

2019 REPORT

Intelligence needs to be applied across all three elements of any transaction: tracking the goods moving in one direction, the payment moving in the opposite direction, and data moving in both directions. Prompted by GDPR and regulations around bribery and anti-money laundering, firms have been seeking to get a better handle on their data and payments – given the volume of transactions, the smart ones have adopted artificial intelligence (AI) to sift through them all efficiently. The 'Cinderella' element in the equation has always been the tracking of goods where few organisations have adopted a smart approach to logistics and inventory.

The really smart approach though, is to be able to apply AI across all three. With audit resources limited, there is a real need to be able to easily and accurately spot anomalies in the flow of goods, payments or data. AI-enabled big data analysis across all three can provide quicker and more accurate identification of potential issues for further investigation. At some point in the future, we will look back and wonder why we didn't always do it this way.

BILL MEW
DIGITAL ETHICS CAMPAIGNER AND CEO, CRISISTEAM.CO.UK

Contents

Foreword

By Laurent Colombant, Continuous Compliance and Fraud Manager at SAS

Procurement fraud can emerge in any organisation that fails to acknowledge and address it. This is why procurement and other forms of internal fraud are such a menace. Many organisations are in denial over the scale of internal fraud, leading to belated investigations that fail to uncover its true extent. While fraud is primarily an external threat, half of all cases are assisted by employees.[1] It is time for businesses to unmask the enemy within.

So long as fraud remains taboo, it will be impossible to eradicate. The first step in overcoming the stigma is to understand you are not alone in being defrauded. Even businesses making genuine efforts to fight back may struggle to keep on top. Their efforts will come up short if they rely on outdated processes, technologies and their own biases.

Successful fraud prevention is a two-stage process. First, organisations must look hard at their current prevention regime and modernise their detection framework. It's important to be proactive. Assume that fraud and error will happen. With the right mindset, procedures and basic business rules in place, stage two can begin – implementing data analytics to ensure accuracy and speed of response. With this approach, it's possible to not only catch fraud, but to prevent it from happening at all.

1. PwC, Pulling fraud out of the shadows, p.9 (2018)

INTRODUCTION

A Wolf in Sheep's Clothing

While often overlooked, procurement fraud is one of the most common and insidious forms of fraud an organisation can encounter. Since 2014, PwC has listed it as the world's second most commonly reported economic crime ranking above bribery, corruption and cybercrime.[2]

There can be many reasons behind fraudulent activity. From lucrative contract wins to disgruntled employees, there is no 'standard' behaviour for organisations to watch out for. The more senior the perpetrator, the more damaging the result is likely to be: executives who engage in occupational fraud cost their business over 10-times more than regular employees.[3]

Procurement fraud lowers revenues, ruins reputations and distracts from the crucial work of businesses. What's worse is that it usually hides in plain sight. Often committed by known suppliers and those closest to the organisation, procurement fraud is estimated to place up to five per cent of business spend at risk each year.[4]

Beyond the bottom-line loss, many jurisdictions impose a mass of regulatory and compliance requirements that can lead to reputational damage and fines if not respected. Regulations, such as the UK Bribery Act (2010) and French Sapin II (2017), oblige companies to perform proper investigations into procurement and hold their employees to high ethical standards.

A lack of awareness and insight around procurement fraud likely masks its true extent. Following the emergence of increasingly competitive tender practices, procurement fraud has become more embedded and harder to detect. The increase of data that organisations have access to, including supplier and auditing information, has also made it more difficult to detect the early warning signs.

2. PwC, Economic crime: A threat to businesses globally, p.6 (2014)
3. ACFE, The Staggering Cost of Fraud
4. ACFE, Report to the Nations, p.4 (2016)

In 2017

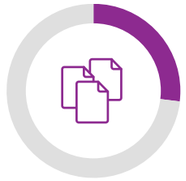
Swedish telco Telia Company AB agreed to pay regulators a **penalty of $965m** after being found in breach of the US Foreign Corrupt Practices Act of 1977. Management and various employees within Telia and affiliates had paid approximately €331m in bribes to the relative of a government official in Uzbekistan to secure public contracts.

CHAPTER 1

Hidden Dangers

THE MOST COMMON FRAUD TYPES

39%
TRAVEL AND EXPENSES



27%
DUPLICATE INVOICING

25%
CONTRACT BID RIGGING

Procurement fraud comes in many forms and is only one of the many types of internal fraud that threaten organisations. To gauge its prominence, and the extent to which business leaders regard it as a threat, we asked respondents to consider a variety of fraud types and report on what they had experienced.

Perhaps unsurprisingly, employees are the most likely culprits. Occupational fraud, the use of one's occupation for personal enrichment through the deliberate misuse or misapplication of the organisation's resources or assets, emerged as the most widely experienced form of fraud. Travel and expenses fraud committed by employees was the most common example, reported by 39 per cent of employers.

Occupational fraud is widely experienced by organisations. Yet, while detection can be difficult, companies usually have all the data and records they need to investigate – something that cannot be said of external suppliers. Expenses fraud, for example, is well understood and front-of-mind in many fraud prevention strategies. This laser focus on individual cases of small-scale internal fraud, however, could well be detracting attention from other very real threats on a much larger scale.

FRAUDSTERS MOVE IN HERDS

When an organisation lacks the means to defend itself from fraud, it often falls victim to all kinds at once.
After an investigation, a single bank discovered:

21
EMPLOYEES WITH DIRECT INTERESTS IN SUPPLIERS

120K
CASES OF DOUBLE INVOICING

22
EMPLOYEES SHARING INFORMATION WITH VENDORS

40
CASES OF SUPPLIER COLLUSION

Many types of procurement fraud were similarly prominent in our survey. The most common fraud committed by vendors is the practice of submitting duplicate invoices, experienced by 27 per cent of organisations. More than one in 10 companies (16 per cent) have experienced collusion and secret agreements between suppliers, or between suppliers and employees. A similar number have been defrauded by ghost vendors (13 per cent). Perhaps most surprisingly, contract bid rigging has been experienced by a quarter of all organisations.

Most of these fraud types threaten hefty fines and jail sentences if discovered. Yet regardless of the penalties involved, fraudsters appear willing to take the risk. Both internal and procurement fraud is endemic, so prevention teams can't afford to take their eyes off employees or vendors. Yet what's most compelling from the findings isn't how widespread a particular type of fraud is, but how common they all are. With an even spread across most categories, fraud has become an enemy that can attack organisations from all sides.

The true cost of procurement fraud

Putting a number or percentage on the amount businesses lose from procurement fraud is challenging. For one thing, the extent and scale of the crime is rarely fully known in an organisation. A company may be unaware of procurement fraud going on in the background, but it's still costing them money.

More significant, however, is that the losses do not stop once the fraud has been identified and resolved. Good businesses depend on a good reputation. Russell 1000 index companies considered 'ethical' achieved a seven per cent higher return on equity than their counterparts in the last five years.[5] Revelations of fraud can tarnish this.

The fallout from reputational damage can include lost customers, as well as senior leadership teams being distracted from their work by legal battles. All of these factors can have a damaging and long-lasting effect. In a worst-case scenario, a company victimised by procurement fraud could well lose precious market share that takes years to regain.

When asked how much they lost due to procurement fraud and processing errors, the most common amount – selected by 26 per cent of businesses – fell in the range of $10,000 and $150,000 per year. Just over one in 10 (12 per cent) fell into the $150,000 – $400,000 category, and four per cent claimed a loss of more than $400,000 a year. The amount lost by each respondent will be heavily influenced by the size of the company and the amount it spends on procurement.

Nevertheless, these are significant and unnecessary losses for any company. Between 2015 and 2016, the UK private sector spent almost £2.6 trillion on procurement, significantly more than the country's GDP at the time.[6] It's clear that the procurement of goods and services accounts for a large share of organisational expenditure, and an estimated 4.8 per cent[7] could be saved if fraud were removed from the equation.

It should be emphasised that responses only reflect known losses. The true scale of financial damage caused by procurement fraud could be much larger, though it is masked for a variety of reasons. A great deal goes undetected, unreported or is dismissed as reporting error. For the wrongdoing that is discovered, some victims or colleagues of the perpetrators may feel pressured not to admit the true scale of the fraud or its cost to protect their company's reputation.

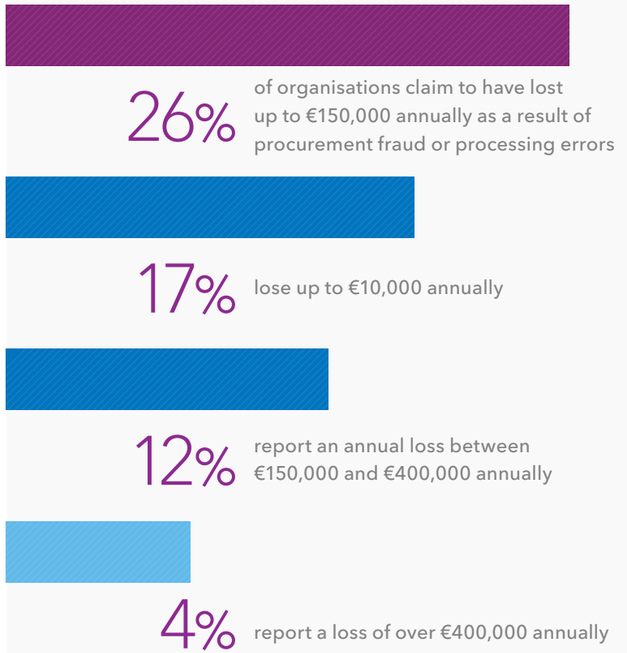
Most concerning are the companies that make little attempt to estimate losses from procurement fraud. Almost a quarter (23 per cent) of respondents believe losses due to procurement fraud are negligible but are unable to specify an exact amount. A further 17 per cent have no sense of how much they lose. That 40 per cent of companies are unable to calculate exact losses from procurement fraud suggests a culture of ignorance or negligence towards the problem. In such an environment, actual losses are likely to be much greater than what's reported.

5. Just Capital, Looking for strong returns? Ask the American people, p.5 (2018)
6. Crowe, Annual Fraud Indicator 2017, p.10 (2017)
7. Crowe, Annual Fraud Indicator 2017, p.11 (2017)

NO LAUGHING MATTER

Losses due to procurement fraud can be devastating. Money overspent on a fraudulent supplier can tie up much-needed investment in other areas and pull down revenues. One large public utility company discovered approximately US $700 million in duplicate invoices alone. The impact and prevalence of procurement fraud should never be underestimated.

How much money is lost due to procurement fraud or processing errors?



CHAPTER 2

An Uncomfortable Truth: Who's Responsible?

As with any business function, clearly defined ownership is needed to successfully tackle procurement fraud. There should be dedicated personnel assigned solely to the task, and it should be clear where final responsibility lies. When accountability is dispersed in a company or fraud prevention is just another role to be juggled, red flags are missed, and fraud falls through the cracks.

Organisations still have much to learn in this respect. In our survey, there was no clear leader or common approach to procurement fraud prevention across businesses. Overall responsibility for dealing with fraud in procurement differs considerably between companies. Indeed, almost a quarter (23 per cent) of business leaders have no clear owner assigned to the task or can't say who is responsible.

The CFO or head of finance position is the most likely role to lead anti-fraud efforts, with almost a third (31 per cent) assigning them responsibility. Yet, the majority of companies give responsibility to other, more diverse functions. The head of procurement was the next most popular option (19 per cent), followed by internal auditors (16 per cent), business or departmental heads (15 per cent) or legal (13 per cent).

Over one in 10 (11 per cent) claim responsibility is shared between departments.

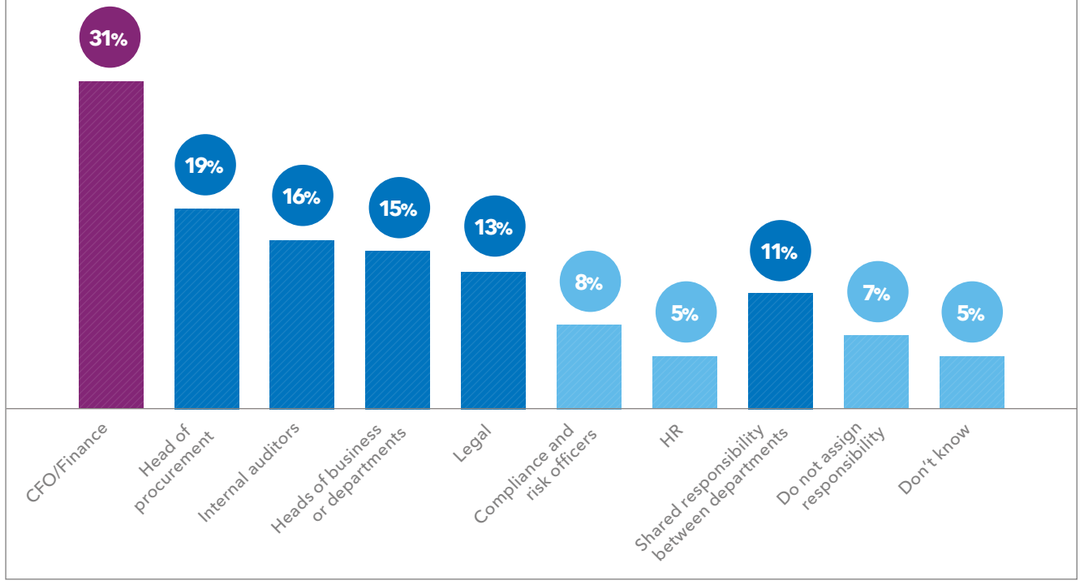
It's important to stress that, while the finance function was the most frequently cited option, the CFO is unlikely to be involved in day-to-day anti-fraud activities. It's probable that they instead hold ultimate responsibility when fraud impacts the financials of their organisation. This is certainly the view of many regulators. In 2014, for example, Sino-Forest Corp. CFO David Horsley was fined C$700,000 by the Ontario Securities Commission for failing to prevent fraud under his watch.[8]

Many of the options chosen by respondents may not be the optimal personnel for the job. This could well be due to lack of resources and necessary skills or potential conflicts of interest. Finance departments may not always first approach procurement from an ethical or accountability standpoint, but instead may be focussed on which suppliers can offer the best deal.

The absence of a common approach suggests that organisations underestimate the likelihood/extent of procurement fraud, or feel they lack the resource or tools to fight it.

8. Ontario Securities Commission, Proceedings 2014-07-21 (2014)

WHO IS RESPONSIBLE FOR DEALING WITH POSSIBLE FRAUD IN PROCUREMENT? (MULTIPLE CHOICE)



Yet, as shown by how damaging fraud can be to an organisation, this position is not sustainable in the long term.

Responsibility for fraud in the workplace is a delicate balancing act. Overall responsibility and strategic decision-making are crucial, but all activity shouldn't be siloed in one department. Instead, fraud accountability and responsibility should be embedded throughout the workplace.

Every employee in every department should be vigilant and encouraged to come forward with their suspicions. For medium-to-large organisations, a dedicated fraud team tasked solely with the detection and resolution of potential fraud is strongly advised.

Do companies take procurement fraud seriously?

An audit or official investigation into a company's accounts can uncover error and potential wrongdoing during procurement. It plays a crucial part in the fight against procurement fraud. How frequently a company undertakes audits can be a useful indicator for its awareness of the threat and its willingness to see it resolved. Another indicator is whether or not procurement fraud analysis is part of the yearly audit plan.

If frequency matches intention, there is much room for improvement. Almost half (46 per cent) of businesses claim to hold regular internal audits, but many exclude internal fraud from their remit. The frequency of audits that included procurement fraud varied considerably between respondents. Annual checks proved to be the most popular timescale, as practiced by a fifth of organisations. Slightly less (15 per cent respectively) undertake audits bi-annually or each quarter. Five per cent hold them ad hoc as needed.

Ultimately, the majority of respondents process a maximum of one or two audits and supplier diligence checks a year, regardless of the number of contracts they offer and secure. This is not as regular as it needs to be. Procurement fraud can be a one-off occurrence or a pattern of wrongdoing that persists for years. Both can be easily timed to evade a well-known annual audit and, even if discovered during auditing, will have already taken their toll on the business.

Worryingly, over one in 10 (11 per cent) organisations admit to either doing nothing to audit for procurement fraud or are unable to say what they do. A further quarter (22 per cent) fail to audit for procurement fraud at all. That one in three companies aren't actively searching for procurement fraud, or don't know what processes cover it, suggests a blind spot that potential fraudsters could easily exploit.

Other areas of the auditing process are also lacking. When we look at how organisations deal with procurement fraud, 29 per cent validate procurement applications manually to minimise mistakes or fraud while a further 30 per cent rely on staff to inform them of any wrongdoing. Both carry a high risk of human error and culpability, potentially minimising or masking the true scale of the problem.

In fighting procurement fraud, process is everything. An over-reliance on human investigators, procedures and the infrequency of investigations, is certain to have a large impact on the success of detection. The larger the gap between audits, the longer procurement fraud will take to be spotted and the less reactive a company will be. This means ongoing fraud is less likely to be detected in progress, making any losses larger and more probable. Organisations should consider a new approach, based on automated, continuous and autonomous detection. This is only possible with a strong foundation of advanced analytics assisting investigators to pinpoint the needles in the haystack.

Should you outsource responsibility?

A small but significant number (13 per cent) of businesses are outsourcing the entire assessment process to external auditors. This strategy holds both advantages and risks. External auditors are more likely to be objective than employees and won't downplay errors or irregularities. They will also be more detached from internal office politics and are more likely to view all employees with an equal level of scrutiny.

> **13%**
> of businesses are outsourcing the entire assessment process to external auditors

However, outsourcing could also be seen as a form of denial or a relinquishment of responsibility. Internal stakeholders and anti-fraud personnel are likely to lose a level of oversight in the process. Businesses must also spend added time to look carefully at the credentials and history of a potential auditor. The Federal Deposit Insurance Corporation attributed blame to the auditors of Colonial BancGroup Inc. before its collapse, and ordered a fine of $625m in 2018 for failing to detect fraud during the auditing process.[9] Even when outsourcing procurement fraud detection, supplier due diligence is essential.

9. Wall Street Journal, damages order for Colonial & FDIC v. PwC

CHAPTER 3

Selecting Suppliers: What Matters Most?

A wide range of competing interests and viewpoints goes into every purchase decision. It's no different when organisations select a vendor or supplier. Going into procurement with the right mindset and priorities can help companies make the right choice, and not just from a financial perspective. To avoid procurement fraud, businesses must expect the same ethical standards from suppliers as they do their own employees. What's more, they need to investigate to be certain.

> One in 10 respondents considered a supplier's history of fraud or errors (10 and nine per cent respectively) as the most important procurement consideration

When choosing a new supplier, companies consider quality of product or service, cost and industry recognition to be the most important factors in their decision.

It's unsurprising also that current suppliers have an advantage over new ones, with respondents selecting this option as their fourth most important consideration and 13 per cent designating it as their top priority.

However, there is a small but significant minority of businesses that place integrity above all else. One in 10 respondents considered a supplier's history of fraud or errors (10 and nine per cent respectively) as the most important procurement consideration. While each procurement scenario will be different, with unique considerations each time, a history of wrongdoing should always be taken into consideration.

The concern of some with procurement integrity is not broadly reflected in wider auditing practices. Similar to internal auditing, supplier due diligence is performed sporadically. The majority of organisations (23 per cent) schedule two due diligence checks a year, followed by quarterly investigations (22 per cent) and annual checks (19 per cent). Only seven per cent conduct supplier due diligence checks every time they start a new project or transaction, and five per cent every time they onboard a new vendor. Many companies only conduct basic checks when onboarding the supplier.

A comprehensive supplier due diligence process should sit at the heart of every project or transaction. The longer organisations wait to perform a check, the greater the chance they will be deceived. A year or even three months is too long to wait and increases the chance of your company entering into a contract with a suspect supplier. Instead, businesses would benefit from a process that analyses the market constantly, vetting vendors and highlighting the risk of fraud before it can begin.

It's understandable that fraud and reputation aren't the top priorities for organisations during procurement. However, carefully vetting a supplier with connections to past or current employees could minimise exposure. Caution and investment at the procurement stage help prevent procurement fraud further down the line. With the right solution, it's also possible to perform due diligence without delaying the process.

CONNECTING THE DOTS OF PROCUREMENT FRAUD

What are the red flags to look out for?

High velocity of address or bank account number changes

The sharing of information, including account numbers, between a third party and employee

Anomalous sequences between invoicing and payments

Duplicate documents

Employees with controlling interests or shares in third-parties

Incorrect or incomplete VAT numbers

CHAPTER 4

Why are Organisations Failing to Spot Procurement Fraud?

Beyond auditing and procurement practices, detection capabilities make perhaps the largest contribution to defending an organisation from fraud. The technology a business equips its staff with to detect the warning signs is a crucial investment.

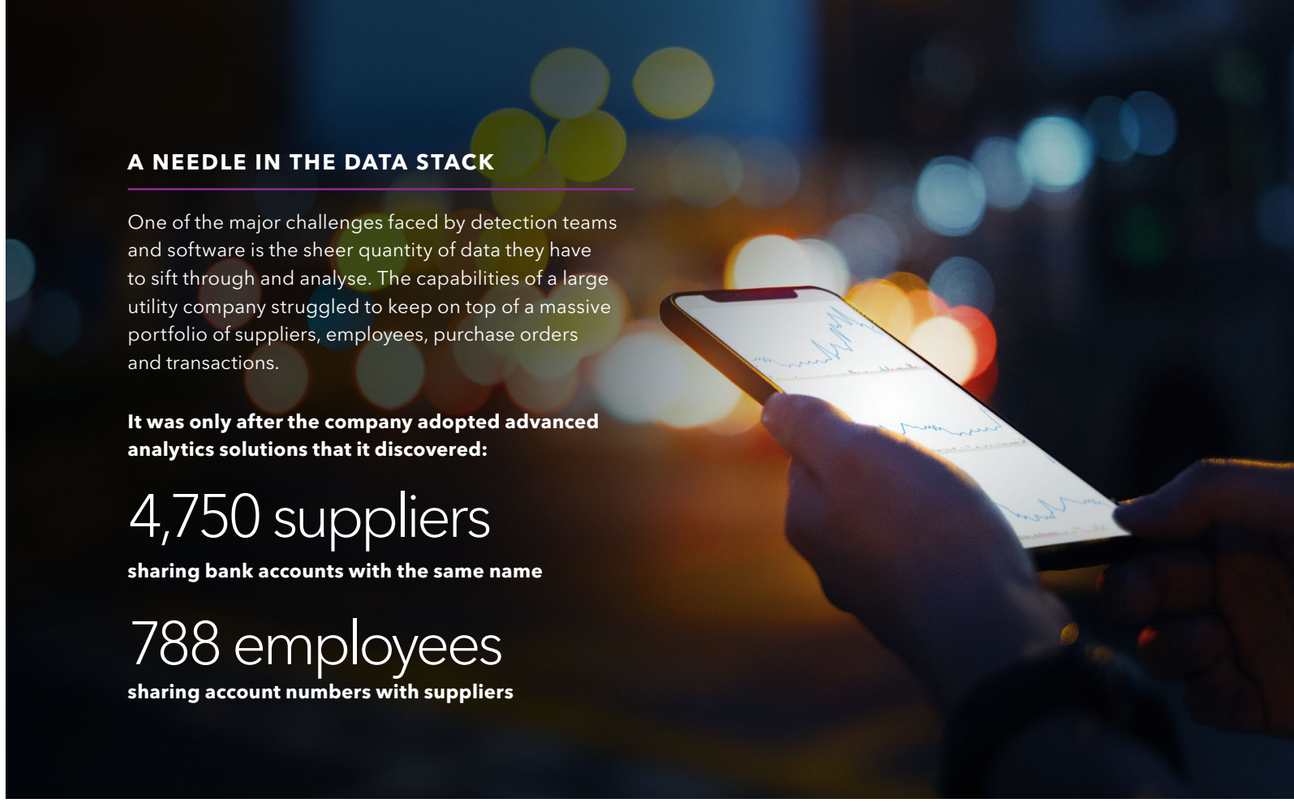
While some organisations fail at fraud detection by not looking for it, others fall short despite their best efforts. The problem is not a lack of awareness or a denial of the issue, but mainly the capabilities they use for detection. Of those that do actively monitor for procurement fraud, the majority are over-reliant on manual processes (43 per cent) or rule-based detection software (31 per cent). User access controls were also popular options, used by three in 10 organisations (31 per cent).

None of these technologies deliver adequate or persistent protection. Considering the lack of accountability for fraud prevention in companies, it's unlikely those performing manual controls consider it to be their primary role. Inevitably, corners will be cut and other tasks prioritised by these employees, making it easy for fraud to slip through the net.

> 62%
> of internal fraud cases were committed by junior or middle managers[10]

Manual controls also bring human bias into the equation. Fraud can be perpetrated by any employee or business leader, but certain personnel may be popular or senior enough that they avoid suspicion. In the Australian public sector, 62 per cent of internal fraud cases were committed by junior or middle managers.[10] They tend to have been with the company for several years and, therefore, usually avoid suspicion. As these perpetrators also typically enjoy high-level clearance and access privileges, user controls quickly become irrelevant.

10. PwC, Fighting fraud in the public sector IV, p.10 (2016)



A NEEDLE IN THE DATA STACK

One of the major challenges faced by detection teams and software is the sheer quantity of data they have to sift through and analyse. The capabilities of a large utility company struggled to keep on top of a massive portfolio of suppliers, employees, purchase orders and transactions.

It was only after the company adopted advanced analytics solutions that it discovered:

4,750 suppliers

sharing bank accounts with the same name

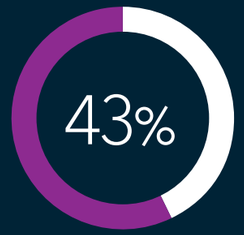
788 employees

sharing account numbers with suppliers

Detection software tends to be more objective, but the implementation is usually rudimentary and rules-based. The technology casts a very wide net, meaning innocent accidents or anomalies are flagged alongside genuine signs of fraud. False positives such as these waste time and resources while real fraud continues in the background. Anyone with knowledge on how the rules behind the software operate could also find strategies to avoid detection.

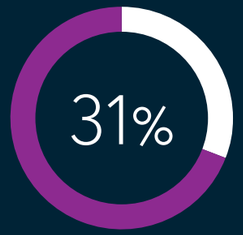
Procurement fraud can occur at any point during the procurement cycle, making it very difficult to investigate. Manual controls only go so far, depending on the detector's skill to detect fraudulent behaviour from within a large set of data. Neither they nor rules-based software can provide the continuous monitoring needed to stay ahead of fraudsters.

HOW DO YOU MONITOR PROCUREMENT PROCESSES FOR FRAUD? (MULTIPLE CHOICE)



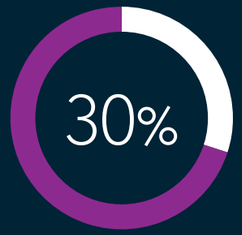
MANUAL CONTROLS

A member of staff manually checks Excel spreadsheets and paper documents for possible errors and suspicious behaviour.



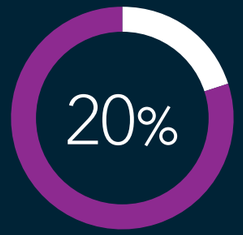
BUSINESS RULES

Software-based technology detects when, for example, somebody tries to send a payment below a threshold or splits an invoice to avoid controls.

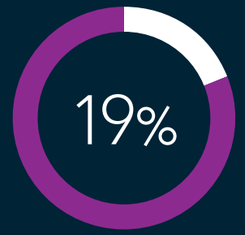


ANOMOLY DETECTION

Software-based tools to detect if a supplier is paying invoices late or at an unusual date outside of the contracted period.

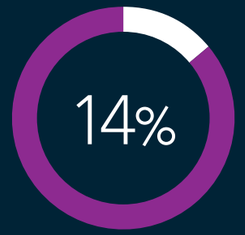


USER ACCESS CONTROLS & SEGREGATION OF DUTIES



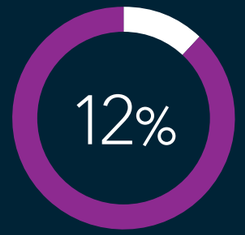
DATA INTEGRATION & CLEANSING TECHNOLOGY

Apply analytics across multiple platforms and operating systems to correlate and de-duplicate data.



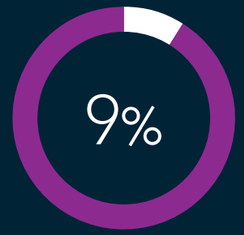
ADVANCED ANALYTICS

Algorithm-based technology, including machine learning, that analyses statistical and text-based information to identify trends and score the level of risk of a supplier, third party, invoice, purchase order and collusions between entities.



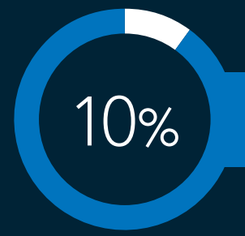
TEXT ANALYTICS

Software-based tools to analyse text data from documents and databases to determine the similarity between two invoices for example.



ARTIFICIAL INTELLIGENCE (AI) & AUTOMATION

The combination of predictive analytics with computer vision and natural language processes to forecast and optimise detection monitoring, with self-learning capabilities.



WE DON'T MONITOR OUR PROCUREMENT PROCESSES

CHAPTER 5

The Untapped Potential of Analytics

When it comes to lacklustre fraud prevention, it's justified for businesses to blame their tools. Current approaches such as manual processes and rules-based software present a fractured front against fraud, full of inherent and structural weaknesses that make them easy to bypass or avoid. What's more, they are unable to cope with the flood of data they must analyse in order to stay ahead of those seeking to commit fraud.

In addition to the tools of detection, business mindsets are also holding organisations back from making the best use of what's available. Continuous, data-driven detection represents the best way to fight procurement fraud and identify errors. It enables companies to pre-empt signs of fraudulent activity rather than discover it after it's taken place, limiting costs, saving time and preventing losses.

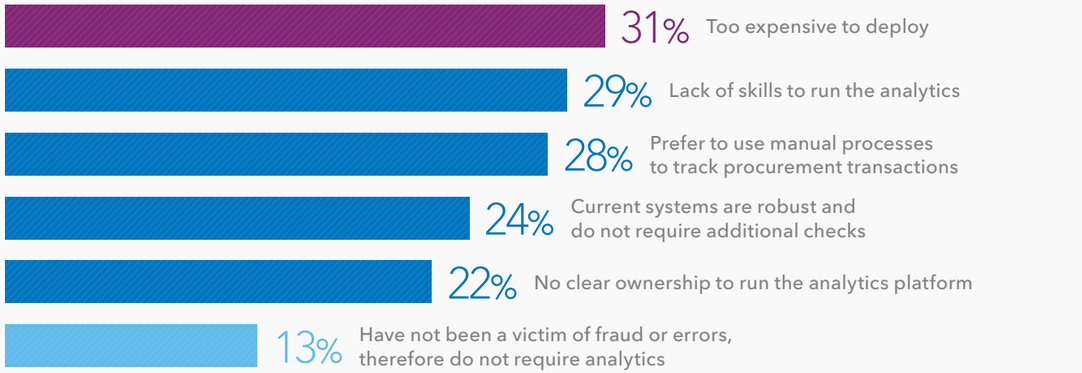
Few companies are using the best tools available to them. A minority are using advanced analytics (14 per cent) and AI (nine per cent) technologies in their anti-fraud efforts. Perceived cost of deployment was the leading reason for companies not to use analytics and AI (31 per cent and 36 per cent respectively).

This was followed by a lack of skills to run the solutions (29 per cent and 30 per cent) and a preference for manual processes (28 per cent and 27 per cent). A significant minority of 13 per cent argued that neither technology was necessary as they had never been a victim of fraud or errors. How can they be so sure?

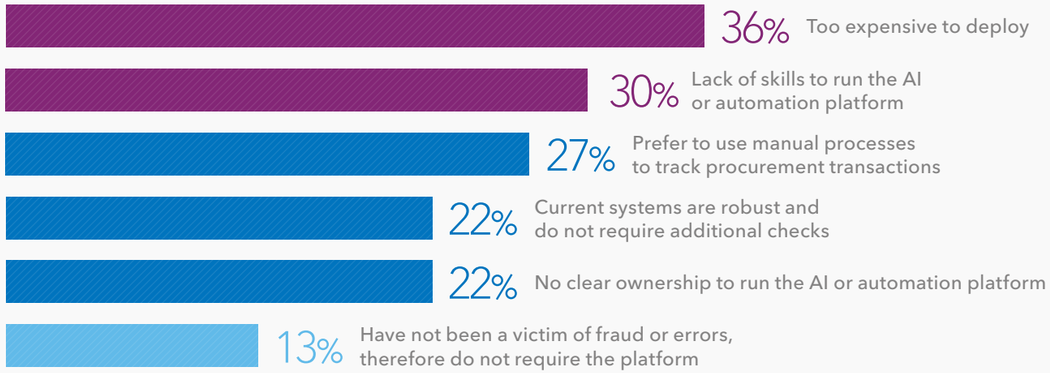
Beyond investing more in the skills that they need, companies will find it difficult to address the chronic lack of data skills apparent in many countries. However, businesses should reconsider their objections to advanced analytics and AI based on cost. Instead, they should evaluate their options based on potential ROI. Implementing the technologies will of course require an upfront cost but will quickly make money for the business in the fraud it detects and prevents. With the average company losing between five-to-seven per cent of revenue to fraud each year, a suitable ROI should not take long to deliver.

Barriers to doing the right thing

THE TOP BARRIERS TO ADVANCED ANALYTICS (MULTIPLE CHOICE)



BARRIERS TO AI



Moving from costs to ROI

To beat procurement fraud, both a long-term strategy and investment in the latest technologies is required. This includes everything from recruitment to upskilling employees and evaluating purchase options based on potential ROI.

One of the great challenges of procurement fraud prevention is the amount of data that needs to be crunched and analysed. Human investigators and basic detection software either cannot do this or will struggle to, but advanced analytics, machine learning and AI have the capabilities to do this quickly and consistently while making money back for the business.

Both advanced analytics and AI are able to pick up on the data points and tell-tale signs of fraudulent activity and alert the business before any damage is done. The crucial insight they then generate from the raw data enables fraud prevention teams to make better, more informed decisions.

By taking up much of the analytics workload and severely cutting down on false flags, a more sophisticated fraud function also frees up significant time for employees. This allows them to spend more time on higher priority alerts.

AI and analytics also help stop procurement fraud up stream and prevent the fraud from continuing. This is a key advantage the technologies hold over other forms of fraud protection. In addition to preventing losses from fraud, being able to demonstrate a proactive approach to preventing corruption may make the organisation more attractive to prospective buyers and customers.

Furthermore, the use of advanced analytics and AI can satisfy regulators in the rare event that a fraud avoids detection, given the company has made the best possible efforts to prevent the fraud from happening in the first place. In addition to a fine, most regulators will also ask that budget be allocated to improving detection software and processes. However, if an organisation can prove that it is already using best-of-breed solutions, then it can't be considered wholly responsible and will likely suffer smaller penalties during fine negotiations.[11]

SPEED IS OF THE ESSENCE

Analytics-enabled modes of detection are much faster than manual controls. As a result, fraudulent activity is uncovered sooner and more quickly, saving considerably more costs in a shorter period of time.

The median duration of internal fraud is 16 months, but the length can vary considerably depending on its type. Payroll fraud for example can continue for as long as 30 months.[12]

11. PwC, Point of View about Risk & Regulatory Technologies, p.2 (2016)
12. ACFE, 2018 Report to the Nations on Fraud, pp.14-15

Last year

a $1.8 billion fraud was uncovered in a South Mumbai branch of the Punjab National Bank which had proceeded unnoticed for seven years. After such durations, the damage has long been done.

By contrast, using data exploration analytics SAS helped a company discover over $50,000 in losses from fraud after only three days.

CONCLUSION

Trust in Data

The majority of organisations are aware of the danger posed by procurement fraud and are taking steps to tackle it. However, thanks to inconsistent audit regimes, an absence of leadership and a failure to utilise the latest technologies, the true scale of the challenge is poorly understood.

What's more, a not inconsiderable minority of businesses are in a state of denial, neither believing they are targets or taking steps to protect themselves from procurement fraud. This naivety is something a potential fraudster could take advantage of. What businesses don't see can still hurt them.

Until organisations adopt an integrated, data-driven approach to detection, millions will continue to be lost to procurement fraud. Companies need solutions able to spot errors and fraud anywhere during the procurement cycle, from bid to contract execution.

Analytic capabilities are crucial to identifying and catching people trying to dodge existing controls and procedures. Detection and investigation tools are also the only way to piece together substantiated cases for prosecution based on the hard facts and data.

By using the latest advanced analytics and AI solutions, anti-fraud teams can sift through huge quantities of data effortlessly. Anomalies and patterns can be detected quickly, enabling businesses to quickly take action. Machine learning models also have the added advantage that they learn over time, meaning they can detect new threats and techniques as they emerge. This is distinct from manual controls and rules-based detection, which take a rear-view mirror approach – analysing old data and patterns retrospectively as opposed to real-time reviews.

Analytics and AI deliver continuous, real-time monitoring, helping audit and fraud teams act in a preventive manner to protect the business and its integrity. With these technologies, procurement fraud can be stopped before it begins. This protects both profits and reputation.

WANT TO KNOW MORE?

Please contact your local SAS office »