FRAUD REVIEW 2019

A review of actual fraud cases in 2018/19

mgi AUDIT & ASSURANCE

Contents

Introduction 3

Fraud Snapshot 4

Case Studies

Key Person Fraud 5

Cyber Fraud – Ransomware 6

Payroll Fraud 7

Expenditure Fraud 8

Outlook for 2019/20 9

Summary 12

Introduction

Fraud costs Australian businesses millions of dollars every year, and these are just the instances that have been detected.

Fraud can occur in any organisation, no matter what size, industry or sector. Fraud has been uncovered in the public and private sectors, in for-profit and not-for-profit entities, and in small, medium and large enterprises.

MGI's audit division helps its clients deter and detect fraud by staying abreast of current fraud cases in Australia. MGI works with clients to implement controls and safeguards to reduce the risk of fraud.

This fraud update is a summary of fraud cases uncovered by MGI Audit & Assurance and other exposed fraud cases in Australia during 2018/19. This update identifies the key factors that permitted the fraud to occur and provides recommendations to reduce the risks of these types of fraud in your business.

Stephen Greene
Director – Audit and Assurance

Fraud Snapshot

60%

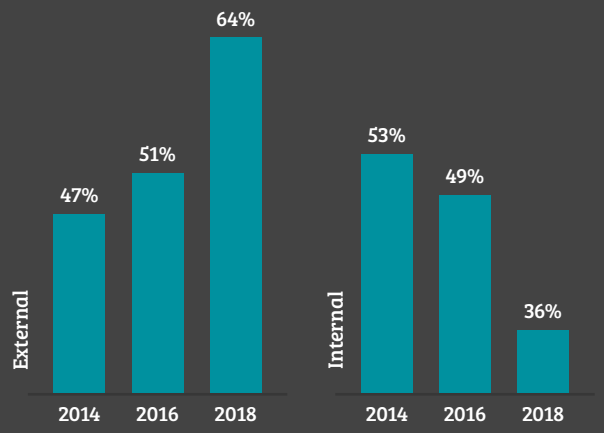
of economic crime in Australia is committed by someone known to the organisation (e.g. employee, consultant, agent, supplier or customer).

43%

of Australian organisations have experienced a cyber attack in the past 12 months.

64%

of fraud were committed by someone external to the organisation versus 36% internal. The proportion of fraud comitted by external fraudsters has grown over the past five years.



64%

of all data breaches in the December 2018 quarter were as a result of malicious or criminal cyber attacks, split across the following categories.

60% Phishing

39% Malware

24% Network Scanning

15% Brute Force Attack

10% Man in the Middle

Source: PwC's 2018 Global Economic Crime & Fraud Survey - Australian Report; Office of the Australian Information Commissioner (OAIC)

Case Studies | Key Person Fraud

Many organisations have a Chief Financial Officer, Finance Manager or Accountant that have been in the role for a number of years. In the majority of cases, the people in these roles are given an unquestioned level of authority and access to the organisation's financial controls. The natural human instinct is to assign a greater level of trust in long-standing employees. However, in certain instances, a greater level of trust can lead to increased opportunities for fraud to occur.

Background

- An executive of a major bank was charged with 56 offences of receiving bribes over a five-year period totalling $5.4 million.
- Offences included maintaining contracts with major suppliers where bribes had been received and approving overstated invoices.
- The executive has been an employee for over 20 years, with nine years as chief of staff to the CEO.

How did this fraud occur?

- There was a lack of internal controls surrounding the procurement of certain contractors that the executive was responsible for, most likely because of the executive's length of service with the bank.
- The executive held a position of advantage that was never questioned.
- Limited review of the profit or loss statement expense codes against budget, given that these expenses would have been recognised in one or more expense codes each year.

Frequency of the fraud risk

- The fraud occurred continuously across a five-year period.

How did this fraud get detected?

- The executive left the position, and irregularities in the treatment of expenditure were subsequently investigated.

How to reduce this fraud risk?

- Implement segregation of duties - no matter the size of the organisation, no individual should have the authority to approve contract terms, invoices and payments.
- Ensure reviews performed by a second person are detailed, and question any items that appear suspicious.
- Ensure all expenses are scrutinised against budget, and any variances are investigated.

Case Studies | Cyber Fraud – Ransomware

Every time you connect to the internet, whether it's from a computer, tablet, or smartphone, you are vulnerable to cyber attacks from outside threats and hackers. One of the most common forms of cyber crime today is known as ransomware, which occurs when a hacker manages to lock and encrypt data on your device and demand a payment in order to release the information.

Background

- The Chief Financial Officer (CFO) received an email purporting to be from the Australian Securities and Investments Commission (ASIC) stating that there was an unpaid company notice, and to follow the hyperlink provided to log in and pay.
- The hyperlink was actually a virus containing ransomware, and the CFO's system and all computers in the system became encrypted.
- The hackers requested USD$25,000 to be paid in bitcoins to unlock the files.

How did this fraud occur?

- Sophisticated phishing email luring the user to click on a link that looked legitimate.

Frequency of the fraud risk

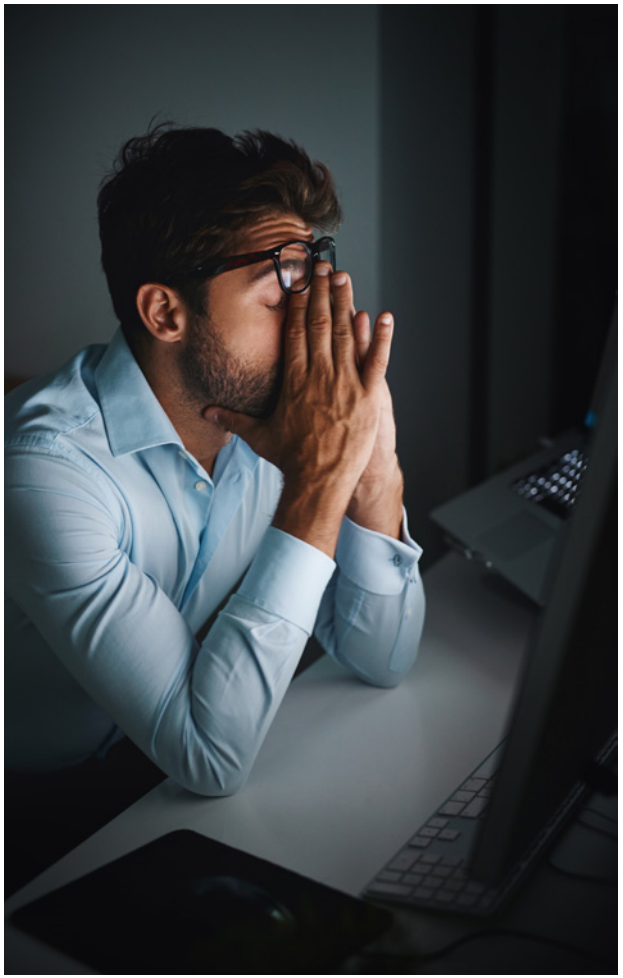
- One click - that's all it took for the virus to be installed and the files encrypted.

How did this fraud end?

- Unfortunately for the organisation, their IT back up controls were not robust enough for a full system restore. The organisation estimated that the ransom price was a lower costs than the cost to manually restore the data, so the ransom was paid.

How to reduce this fraud risk?

- Conduct a full IT system health check of all of your current IT systems.
- Train your staff on cyber fraud risks, including how to spot a phishing email.
- Ensure the most up to date phishing email detection software is installed on all systems.



Case Studies | Payroll Fraud

According to the most recent Australian Payroll Association's Payroll Benchmarking Survey of more than 20,000 employers, Australian Organisations are making on average $50,000 of payroll errors annually... and these are just the ones the employers find out about.

Background

- Involved the payroll clerk of a large charitable organisation. The payroll clerk had been with the organisation for more than 10 years.
- The payroll clerk had full autonomy to run payroll transactions, change pay rates, add new employees, and transact leave entitlements.
- In any instance in which an employee requested unpaid leave, the clerk would put through normal hours into the payroll system for that employee, but make wages be paid to a fraudulent bank account they had set up.
- The same was performed for employees on maternity leave.
- The payroll clerk would change the bank details back to the employee's bank details once they returned from unpaid/maternity leave.

How did this fraud occur?

- Whilst this was an elaborate fraud, no controls were set up to reconcile unpaid leave requests to the payroll reports, to identify anomalies.
- Over-reliance on one payroll clerk to have access to all areas of the payroll process, without a second review (e.g. bank account changes).

Frequency of the fraud risk

- On every weekly payroll in which an employee took unpaid leave/maternity leave.
- While this fraud is internal, it is likely that this fraud would continue to occur until detected, or until the employee left the organisation.

How did this fraud get detected?

- The payroll clerk forgot to change one of the employee's bank account details back to their actual bank details, and therefore queried the General Manager when their wages were not received on pay day. A full investigation was then launched .

How to reduce this fraud risk?

- Ensure segregation of duties within payroll processes.
- Implement spot-checks of individual pay-runs, ensuring a sample of employee details are vouched back to their employee file (including pay rates, bank account details, etc.).
- Implement controls reconciling unpaid and maternity leave employees to payroll reports.

Case Studies | Expenditure Fraud

Certain situations increase the likelihood of fraud, such as when a trusted employee is given the authority to make significant purchases with little to no scrutiny.

Background

- Involved a large charity in Victoria.
- The General Manager (GM) submitted renovation invoices on their personal property to the Finance Manager for approval, totalling $176k.
- The renovation invoices were not queried, as the charity was also undergoing renovations at their head office.
- The GM also incurred $27k worth of personal expenses on the charity's corporate credit card.

Frequency of the Fraud Risk

- 45 personal renovation invoices were submitted and paid over a six-month period.
- Personal credit card expenditure was being incurred on the corporate card for a number of years.

How did this fraud occur?

- Whilst second reviews of these invoices were apparently occurring, they were not sufficient enough in order to detect obvious anomalies (e.g. swimming pool installation for a charity)
- Too much trust was placed on one individual.

How did this fraud get detected?

- During a fixed asset count, anomalies were noted in the assets on the fixed asset register. Upon querying the building contractor, it was noted that the asset installation occurred at the then GM's house.

How to reduce this fraud risk?

- Second reviews of creditors payments are completed with sufficient detail, requiring the reviewer to have access to the supplier invoices to query any unusual transactions.
- Ensure the second reviewer chosen is of sufficient seniority - in this instance the Finance Manager was outranked by the GM, so may have been intimidated to query any unusual transactions. It may be advisable to have a Board member review.

Outlook for 2019/20 | Are your IT controls robust enough?

While the rates of cyber fraud are already alarmingly high, the Australian Government estimates that all types of cyber fraud will continue to rise, and become the "new norm".

Especially at risk are small and medium-sized businesses according to the Reserve Bank's Cyber Security Chief, who believes fraudsters are turning their attention to "easier prey" at the smaller end of town.

Smaller businesses are less likely to take cyber fraud risks as seriously as larger listed organisations, and therefore likely to have weaker preventative controls against common cyber fraud techniques such as email phishing, ransomware and identity theft to name but a few.

While cyber fraud attempts are now unfortunately inevitable for most Australian businesses as we move into 2019/20, it is essential that all organisations understand the risks of cyber fraud and plan accordingly.

The key areas we advise our clients to consider with regards to cyber fraud are as follows:

Have Your IT Controls Tested

An IT Health Check is a low cost assessment of your current IT controls, which will highlight any potential risks your organisation is currently exposed to, including the risk of external hackers obtaining access to your private data. This will cover such areas as data back up procedures, disaster recovery testing, penetration testing of your website and servers, higher level assessment of current software and hardware deployed, and user access rights.

The MGI IT division are available to conduct an IT Health Check of your IT systems in order to ensure your organisation is protected.

Education and Training

Most employees of small and medium-sized business are acutely unaware of the risks that may unfold if they open a fake speeding ticket invoice attachment from the Australian Police or fake energy bill from Origin. Providing basic training to your staff on the types of common cyber fraud out there will be money well spent in protecting your business from this ever-increasing risk.

Detection and Prevention

Detecting cyber fraud and implementing controls to prevent future attacks is essential in the war against cyber fraudsters.

Detecting cyber fraud starts with implementing and documenting detailed internal financial and accounting controls. Remaining vigilant and questioning all variations to your internal policies will highlight that bogus request from a supplier to change bank details, or the email request to transfer money to a designated account.

In addition, your IT policies and procedures must have standard controls such as regular penetration tests, sophisticated user passwords and phishing detection software to detect any cyber breaches.

IT controls should also cover preventative measures, such as sufficient and up to date virus and firewall software.

Outlook for 2019/20 | Are your IT controls robust enough?

Disaster Recovery

If the first two areas fail, then having sufficient disaster recovery systems is essential to reduce business disruption and loss of data.

For example, if back ups are being taken to a cloud server every 15 minutes and an employee accidentally opens a phishing email with a ransomware attachment, the business can be up and running on the back up version within the hour with only minimal loss of data.

Disaster recovery is, therefore, the final line of defence in an ever-increasing cyber fraud environment.

Key tips when reviewing your disaster recovery systems:

Ensure your disaster recovery system is documented in a jargon-free policy that all the Principles of the business can understand and follow. If your IT Manager is on a beach in Florida when a cyber fraud event occurs, there needs to be a second option.

Ensure your data back ups occur regularly. Having backs ups only occurring once a day still leaves your business open to business disruption in the event of an attack. We recommend back ups should be taken as regular as possible to reduce this risk.

Test your disaster recovery process! We recommend testing a full system recovery at least annually. If you have external IT providers, ensure they are testing this and providing confirmation reports on the success of the restoration regularly.

Outlook for 2019/20 | Are your IT controls robust enough?

Data Breach Legislation

In 2018, the Federal Government's new mandatory data breach notification laws came into effect. These new requirements involve fundamental changes to how organisations handle personal information, and organisations need to reconsider how they handle personal information to avoid breaching rules and risking significant fines.

Who must comply with Data Breach Legislation?

Agencies and organisations (entities) that already have obligations under the *Privacy Act 1988* (Cth) to secure personal information must comply with legislation. This includes, for example, businesses that have an annual turnover of more than $3 million, and entities that trade in personal information.

How can you prepare?

Businesses of all sizes are potential targets for data breaches. Whilst IT systems are an important factor in remaining compliant with data protection, data breaches can still occur through human error, mischief, or simply because those looking for ways to disrupt are often one step ahead.

While IT security is a significant consideration in preparing for these changes, businesses should also consider people policies and processes, as there have been numerous cases of physical data breaches, such as hard copy records being disposed of inappropriately, employees allowing malware and viruses to penetrate servers after opening seemingly secure emails, and sensitive data exposed through lost USB drives.

Given the wide-ranging impacts of these new laws, MGI strongly recommends that its clients immediately review their IT processes, policies and security measures to ensure their systems are up to date, people are trained and that a data breach response plan is in place.

Please feel free to contact us if you need assistance with ensuring your organisation is complying with Data Breach legislation.

Summary

The level of sophistication of current day fraud requires boards and management to improve their internal controls and ensure their organisations are well placed to deter and detect fraud.

Fraud can occur in any organisation, no matter what size, industry or sector. Fraud has been uncovered in the public and private sectors, in for-profit and not-for-profit entities, and in small, medium and large enterprises.

Our recent experiences with fraud has highlighted IT risk as the fastest growing fraud risk for organisations, due to the increasing reliance on information technology, paperless financial systems and cloud-based software. This increasing reliance has also increased the fraud opportunities to target businesses whose IT controls have not been upgraded to match their usage.

It is essential that your organisation implements and documents sufficient internal controls to prevent and detect all potential types of fraud that may impact your business. This starts by having experienced auditors assisting your organisation to highlight all potential fraud risks.

Speak to one of our team today about our free IT Cyber Fraud Health Check, which will uncover any potential weaknesses to your current cyber fraud controls and recommendations for improvement.

Get in touch

Stephen Greene
Director – Audit and Assurance

Mobile 0426 510 812
Email sgreene@mgisq.com.au

Graeme Kent
Director – Audit and Assurance

Mobile 0414 828 812
Email gkent@mgisq.com.au

mgi AUDIT & ASSURANCE

This publication contains general information only and MGI Audit and Assurance is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your organisation. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor. MGI Audit and Assurance shall not be responsible for any loss sustained by any person who relies on this publication.