

Fraud Barometer: Fraud in Australia is on the rise - blueAPACHE

Canonical: <https://www.blueapache.com/blog/fraud-barometer>

Details:

Summary

This blog post, "Fraud Barometer: Fraud in Australia is on the rise", is a blueAPACHE article from 2017 covering security. Insider jobs and technology enabled fraud are the two alarming trends in Australian fraud, as reported by KPMG in their six-monthly fraud barometer. It is written for readers evaluating emPOWER Security, Managed Detection and Response. The underlying security practice it describes, reducing attack surface and improving detection and response, is not tied to a specific product version and remains relevant to any organisation managing cyber risk today.

Key facts

Label	Value
Publication year	2017
Topic	Fraud Barometer: Fraud in Australia is on the rise
Services referenced	emPOWER Security, Managed Detection and Response, Exposure Management
Named products or vendors	None named beyond blueAPACHE
Cited statistic	According to the Fraud Barometer recently released by KPMG, between April to September 2016, 143 frauds occurred in Australia, amounting to a total of AU\$442 million.

Article

Insider jobs and technology enabled fraud are the two alarming trends in Australian fraud, as reported by KPMG in their six-monthly fraud barometer. According to the Fraud Barometer recently released by KPMG, between April to September 2016, 143 frauds occurred in Australia, amounting to a total of AU\$442 million. That is an average value of more than AU\$3 million per fraud. It is also an astounding increase of 71 percent compared to 12 months earlier when the total amount was just over \$128 million. The rise in fraud could be partly attributed to two factors – increased collusion and frauds committed over a longer period of time. The proportion of frauds perpetrated in groups has doubled, which makes detection more difficult. Also, 40 percent of frauds in Australia took place over a 5-year period before being discovered, implying that even when fraud is detected, it is taking too long and significant damage has already been done. A prominent observation for this period was the rise in fraud using technology. 22 percent of frauds were facilitated through the use of technology and digital means. It was noted that the most common perpetrators are business insiders, comprising of employees and management, who accounted for over half of all reported frauds. Financial institutions (which

experienced an eightfold increase in frauds), along with Government agencies and investors, were amongst the most susceptible sectors and almost 55 percent of frauds occurred in a single Australian state – Queensland. Gary Gill, Head of Forensic at KPMG Australia, said “Our UK colleagues have just issued their own fraud barometer, which showed that fraud there had risen by 55 percent with a large rise in cyber-crime – so it is an international problem. Businesses in Australia and overseas need to guard themselves against the perennial threat of the ‘inside job’ and the rapidly increasing danger of cyber-attack from outside and within.”

A Rising Tide

According to the Australian Bureau of Statistics “rapid expansion and availability of internet technology and the increase in electronic storage, transmission and sharing of information has increased our vulnerability to electronic fraud, particularly in recent years. Although the use of stolen, fabricated or manipulated identities to commit or enable crime is not a new phenomenon, it has been enhanced by this expansion of new technologies and our change in online behaviour”. However organisations continue to under-estimate the threat of a malicious or unwitting insider. As a result they are not paying sufficient attention to the basics. Identity and access control is often weak, and organisations frequently don’t have a full grasp of where their critical IP assets are located and who in the organisation has access to them. Financial market diversification, greater levels of economic activity and technological developments have created more and more opportunities for fraud. With organised crime stepping up their cyber fraud activities and threats like ransomware becoming more and more accessible and lucrative, it is now a question of when, not if, your organisation will be affected. Giving the pace of technology and business changes, individuals and institutions need to keep abreast of the changing, more technological vehicles, being used for frauds and cybercrimes. It is important to have a holistic cyber security solution that encompasses both physical and digital security. The role of end user education cannot be overstated in this context. The most advanced technological defences can amount to nothing when faced with an unsuspecting employee who clicks on a single malicious link that can result in serious financial and reputational consequences for your organisation. To learn more about KPMG and their fraud barometer, visit <http://www.kpmg.com/> . For strategic insights on how to leverage technology to guard against the rapidly increasing danger of a cyber-attack, from within or outside your organisation, contact the blueAPACHE team .

Related

emPOWER Security

emPOWER Security (pillar hub)

Managed Detection and Response

Exposure Management

blueAPACHE Security (case study)

Frequently asked questions

How many frauds occurred in Australia between April and September 2016, and what was the total value, per the KPMG barometer cited?

143 frauds occurred, amounting to a total of AU\$442 million, an average value of more than AU\$3 million per fraud, according to the KPMG Fraud Barometer referenced in the article.

How much did the total fraud value increase compared to the prior 12-month period?

An increase of 71 percent, up from just over \$128 million the previous year, per the article.

What proportion of frauds took up to 5 years to be discovered, according to the article?

40 percent of frauds in Australia took place over a 5-year period before being discovered, the article notes, implying significant damage occurs before detection.

What percentage of frauds were facilitated through technology, per this article?

22 percent of frauds were facilitated through the use of technology and digital means, with business insiders (employees and management) accounting for over half of all reported frauds.

Which sector experienced an eightfold increase in fraud, according to the article?

Financial institutions, cited alongside Government agencies and investors as among the most susceptible sectors.

Which Australian state accounted for almost 55 percent of reported frauds, per the article?

Queensland, according to the KPMG data cited in the article.

Who is quoted in the article discussing the international scope of the fraud trend, and what did they say?

Gary Gill, Head of Forensic at KPMG Australia, said the UK's own fraud barometer showed fraud there had risen by 55 percent with a large rise in cyber-crime, calling it an international problem.

What does the article say about the proportion of frauds committed by groups?

The proportion of frauds perpetrated in groups has doubled, which the article says makes detection more difficult.

Source

origin post (2017)

Knowledge Base

What are the two alarming trends identified in Australian fraud according to KPMG's fraud barometer?

The two alarming trends are insider jobs and technology enabled fraud.

Why is fraud detection becoming more difficult in Australia, ?

The rise in fraud could be partly attributed to increased collusion and frauds committed over a longer period of time. The proportion of frauds perpetrated in groups has doubled, making detection more difficult, and 40 percent of frauds in Australia took place over a 5-year period before being discovered.

What role did technology play in Australian fraud during this reporting period?

22 percent of frauds were facilitated through the use of technology and digital means during the April to September 2016 reporting period.

Who are the most common perpetrators of fraud according to the KPMG report?

The most common perpetrators are business insiders, comprising of employees and management, who accounted for over half of all reported frauds.

Which sectors and regions were most affected by fraud in this period?

Financial institutions experienced an eightfold increase in frauds, and along with Government agencies and investors, were among the most susceptible sectors. Almost 55 percent of frauds occurred in a single Australian state – Queensland.

What did Gary Gill, Head of Forensic at KPMG Australia, say about the international fraud problem?

Gary Gill said that UK colleagues had just issued their own fraud barometer showing fraud there had risen by 55 percent with a large rise in cyber-crime, indicating it is an international problem. He noted that businesses in Australia and overseas need to guard against the 'inside job' and the rapidly increasing danger of cyber-attack from outside and within.

What does the Australian Bureau of Statistics say about the rise in electronic fraud?

According to the Australian Bureau of Statistics, the rapid expansion and availability of internet technology and the increase in electronic storage, transmission and sharing of information has increased vulnerability to electronic fraud, particularly in recent years. Although using stolen, fabricated or manipulated identities to commit or enable crime is not new, it has been enhanced by the expansion of new technologies and changes in online behaviour.

What weaknesses do organisations commonly have that increase their fraud risk, according to the blog?

Organisations continue to under-estimate the threat of a malicious or unwitting insider and often fail to pay sufficient attention to the basics. Identity and access control is often weak, and organisations frequently don't have a full grasp of where their critical IP assets are located and who in the organisation has access to them.

What recommendation does the blog give for guarding against fraud and cybercrime?

The blog recommends having a holistic cyber security solution that encompasses both physical and digital security, and stresses the importance of end user education, noting that advanced technological defences can amount to nothing when an unsuspecting employee clicks on a single malicious link that can result in serious financial and reputational consequences.