KPMG Kundu

June 2024

Foreword

As we reach the midpoint of financial year 2024, it is perhaps a good juncture to unravel what we see as headwinds before us as we charter our path to the end of the year.

The rapid rise in fraud related activities and its cost burden is of grave concern to business and government. We share more information on the types of fraud and the alarming global statistics and costs that have been reported. PNG is not immune to what is already growing roots in the country.

Another challenge facing PNG is our preparedness in the Cybersecurity landscape. We describe this issue as a ticking time bomb – the threat is very real. We highlight the risks actions to counter these threats.

Turning to the Economy, we share recent statistics by Westpac on their forecasts on GDP and inflation for 2024. For those lagging behind with their tax returns, we point out deadlines.

Enjoy the read this month and reach out with any enquiries at kmcentee@kpmg.com.au if you would like to see KPMG cover specific topics in future editions.

Fraud is evolving: Are you ready to stay ahead?

by Giann Carlo Marquez, Manager, Advisory Services

In today's rapidly evolving world, despite technological advancement and increased regulation, fraud and financial crime remain a serious threat to public and private organisations worldwide. Fraudsters try to take advantage of changes in business environments, markets, and technologies to outsmart the system.

Fraud and financial crime can involve many illicit behaviours, including asset misappropriation, customer fraud, financial statement fraud, money laundering, bribery, corruption, cybercrime, insider training, intellectual property theft, and more. If not detected early and addressed professionally, the consequences are expensive and operationally disruptive.

The recent KPMG Fraud Outlook Survey found as follows:

1. It is estimated that the cost of fraud to a bank is four times the amount lost.
2. Money mule activity is increasing by 78% year-on-year.
3. By 2024, US Card payment fraud is set to reach USD 13 billion.
4. There has been a 228% increase in scam losses in Singapore from 2020-2022.
5. STG 4 billion was lost to fraudsters in the UK in 2022.
6. Global online payment fraud is set to exceed USD 343 billion by 2027.

According to Occupational Fraud 2024: A Report to the Nations published by the Association of Certified Fraud Examiners, the total losses from 1,921 fraud cases examined in 138 countries and territories amounted to USD 3.1 billion. It estimates that organisations will lose 5% of revenue to fraud each year. The most common but least costly scheme is the asset misappropriation scheme (89% of cases), while the least common but most costly scheme is financial statement fraud (5% of cases).

In addition to financial loss, in our experience, non-monetary damages such as impairment of brand reputation, alienation of valued customers and suppliers, and diminishment of market confidence and trust can have a catastrophic impact on an organisation.

PNG organisations face similar threats. Some of the common fraud risks we have come across in PNG include:

- Employee fraud involving asset misappropriation or theft. This can often involve collusion between procurement, inventory and finance personnel.
- Payroll fraud such as the inclusion of ghost employees, intentional alteration of calculations or rate, and incorrect recording of leave balances.
- Fraud and irregularities across the procurement process, employment, travel, and reasonableness of expenditure in relation to donor funded projects in PNG.
- Collusion between finance team personnel to divert payments to non-existent suppliers.
- Collusion and misconduct involving senior management.
- Misappropriation of fuel using company fuel cards.
- Mis-recording of sales by sales personnel to avail of sales bonuses.
- Bribery and corruption.

Less common in PNG but still possible are insurance fraud and identity theft.

The above examples are not exhaustive and some organisations in PNG may be susceptible to other fraud schemes. To combat these threats effectively, in addition to having strong anti-fraud controls such as internal audits, robust compliance measures, defined roles and responsibilities, and fostering a culture of integrity, organisations may consider the following fraud mitigants, which can be tailored to the organisation's size and complexity to mitigate the risks linked with fraud and financial crime:

1. **Regular fraud risk assessments:** These assessments identify organisations' fraud vulnerabilities and help prioritise investments in anti-fraud mechanisms. They should be updated frequently to account for significant changes in the company's legal environment and business operations. A thorough fraud risk assessment is likely to show where the control gaps are.
2. **Fight back with technology:** Technology is a double-edged sword. As fraudsters become more adept at overriding and circumventing controls using technology, organisations can also take advantage of what technology offers to prevent, detect, and respond to wrongdoing.
3. **Know business partners and third parties:** An organisation's fraud prevention framework should extend to cover business partners and third parties conducting business on their behalf. Conducting proper due diligence before entering a business relationship is a best practice.
4. **Tone at the top:** A consistently surprising result in the previously mentioned study and survey is the number of fraudsters who are senior managers who have been with the company for at least six years. Developing a strong culture and tone at the top is essential, led by the organisation's Board of Directors.
5. **Consider investing in Forensic Investigation Services:** Fraudsters may evade or override controls even if they are robust. Investing in a competent fraud risk management team may assist in assessing the nature of fraud and misconduct risk exposures and evaluating program and control effectiveness.

In conclusion, individuals and organisations should remain vigilant in their fight against fraud. As the landscape of fraud and financial crime continues to evolve, organisations should proactively prevent fraud and corruption and mitigate its consequences.

About the author: Giann is a Certified Internal Auditor and Certified Fraud Examiner. He is experienced in assessing internal controls for PNG companies and in performing fraud assessments and fraud examinations.

PNG's cybersecurity landscape: a ticking time bomb

by Happy Ketias, Associate Director, Advisory Services

Papua New Guinea (PNG) is facing a critical cybersecurity crisis and the situation is rapidly deteriorating. Many PNG organizations have failed to patch their servers and address known vulnerabilities, leaving them exposed to devastating attacks.

The looming threat

The majority of PNG organizations rely on Microsoft servers in their IT environment. Microsoft has issued a stark warning, stating that cybercriminals are actively exploiting these vulnerabilities to bypass the Windows operating system's security measures. This means that organizations with unpatched servers are essentially sitting ducks, waiting to be targeted by malicious actors.

Other applications such as Gmail are also being targeted by hackers but as Microsoft is most common in PNG we have focused on this.

Just last week, Microsoft released its regular Patch Tuesday updates to address a total of 149 vulnerabilities across various Windows components. These patches are designed to close security holes and prevent attackers from exploiting them. However, many organizations have yet to apply these critical updates, leaving their systems vulnerable to attack. The update was important to protect against phishing campaigns that could affect individuals, businesses and governments.

In a recent widespread phishing campaign targeting Microsoft customers attackers were able to bypass the Windows security controls and gain access to sensitive information by tricking users into clicking on malicious links or attachments. It also allowed attackers to bypass the Windows security warning when opening files downloaded from the internet. Attackers were using this to send exploits in zipped files.

The knowledge gap

Part of the root of the problem in PNG lies in the significant gap in cybersecurity knowledge and resources. Many organizations simply lack the expertise and the financial resources to keep up with the rapidly evolving threat landscape.

This was a key takeaway from a recent cybersecurity roundtable hosted by Australia's Minister for Home Affairs and Cybersecurity, Ms. Clare O'Neil. The discussion highlighted the unique challenges faced by PNG including:

1. **Resource Limitations**: The country's limited resources make it difficult to build and maintain robust cybersecurity capabilities, leading to a heavy reliance on external support.
2. **Fast Digital Growth:** The rapid expansion of digital infrastructure in PNG has outpaced the development of effective cybersecurity measures, leaving many systems vulnerable.
3. **Cybercrime Prevention:** Strategies to counter the increasing threat of cybercrime and potential espionage are lacking.
4. **Capacity Building:** There is a critical need for training and development programs to empower local cybersecurity professionals and implement effective security strategies.
5. **Collaborative Efforts:** Regional cooperation is essential to enhance cybersecurity resilience across the Pacific, but progress in this area has been slow.

A ticking time bomb

The combination of unpatched servers, known vulnerabilities, and the lack of cybersecurity expertise has created a ticking time bomb in PNG. It is only a matter of time before a major cyber-attack cripples' critical infrastructure, disrupts essential services, and causes widespread damage.

A call to action

The time to act is now. Organizations in PNG must urgently review their cybersecurity posture, patch their servers, and address known vulnerabilities. Failure to do so could lead to devastating consequences, including data breaches, financial losses, and reputational damage. The government and private sector must also work together to develop and implement comprehensive cybersecurity strategies that address the unique challenges faced by PNG. This includes investing in capacity building, fostering regional cooperation, and promoting awareness of cybersecurity best practices.

The clock is ticking, and the threat is real. The PNG cybersecurity landscape is a ticking time bomb, and the consequences of inaction could be catastrophic. It is time to act and secure the digital future of the country.

About the author: Happymabel is an IT professional and cyber security expert. She has been assisting organizations in PNG in addressing critical cybersecurity challenges including incident response. As an expert in the field she can provide guidance on implementing leading cybersecurity practice.

PNG economic indicators and forecasts

Westpac bank recently published a table outlining PNG's economic indicators and forecasts for 2023 to 2025. We found it interesting that 2024 is forecast by all parties to have a higher GDP growth than 2023, while inflation is generally also expected to be higher for 2024.

Economic indicators		2023 (est)	2024 (forecast)	2025 (forecast)
Inflation	ADB	5.0%	5.0%	TBC
	BPNG	3.9%	5.0%	5.5%
	IMF	5.7%	4.7%	TBC
	Westpac	4.0%	5.0%	4.5%
GDP growth	ADB	2.0%	4.5%	4.6%
	BPNG	1.4%	3.0%	4.4%
	IMF	2.9%	4.6%	3.1%
	Westpac	1.5%	4.5%	4.6%

ADB forecasts as at April 2024; BPNG as at March 2024; IMF as at May 2024; Westpac as at May 2024

Income Tax return deadline

If your company has a tax agent, and has a 31 December year end, then this is a reminder that tax returns for taxable companies are due by 31 July 2024 and tax returns for non-taxable companies are due by 31 August 2024. If your company does not have a tax agent, then unfortunately the tax return is already overdue. It is still possible to be added to a tax agent listing so as to avail of the tax return extension but we recommend you act fast.

Our social media presence

As usual, you may access our regular multi-disciplined thought leadership pieces, newsletters, and updates on our KPMG PNG LinkedIn page. Also, connect via our webpage www.kpmg.com.pg and Facebook https://www.facebook.com/pngkpmg/

Contact US

Zanie Theron

SPP PIC
ztheron@kpmg.com.au

Karen McEntee

Partner
kmcentee@kpmg.com.au

Pieter Steyn

Partner
psteyn@kpmg.com.au

Ces Iewago

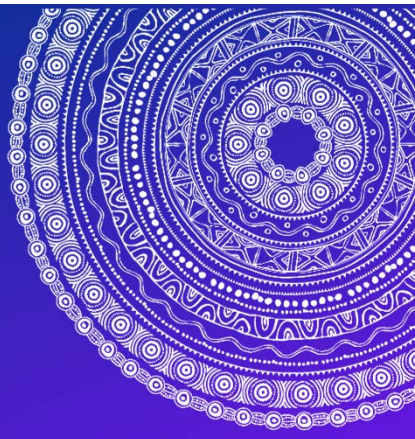
Managing Partner
ciewago@kpmg.com.au

Brett McDermott

Partner
bmcdermott@kpmg.com.au

Christian Angelopoulos

Partner
cangelopoulo@kpmg.com.au



kpmg.com.pg