KPMG Kundu

June 2023

Foreword

PNG is not immune from cybercrime as we see from some very disturbing real-life examples of recent PNG cyber incidents. We have also explored the contents of the new Associations Incorporation Act and what it means for associations. In the IRC space, IRC are stepping up their activity with a door-to-door business mapping exercise in NCD and the recent conclusion of an extensive transfer pricing audit.

KPMG in PNG has dedicated in-house specialists in all the following areas: internal audit/risk, visa migration, corporate finance, management consulting, IT advisory, fraud investigation as well as tax and assurance. As such we are well placed to provide a truly multi-disciplined approach to business advisory.

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.

Ces

Overview of the New Associations Incorporation Act

by Cieran Kelly, Senior Tax Consultant, Business, Tax & Advisory Services

As part of a suite of reforms with a view towards modernising Papua New Guinea's compliance and regulatory environment, Parliament has recently certified a new Associations Incorporation Act 2023 that will repeal and replace the previous Act in its entirety. We understand that the old Act will be repealed a year after the commencement of the new Act, and no new associations can be incorporated under the old Act thereafter.

The primary objectives of the new Act are to improve transparency and governance of incorporated associations and to allow the State to better enforce international anti-money laundering and counterterrorism standards. It will come into operation in accordance with a notice in the National Gazette.

We anticipate that prior to the notice of commencement, accompanying Regulations will be released. These Regulations are expected to cover how forms must be signed, prepared, completed, or submitted. The timelines for submitting documents to the Registrar, the fees for various activities under the Act, including penalties and late fees.

Elements of an association

For an association to qualify for incorporation under the new Act, it will need to establish that it has the following essential elements:

- a lawful name that is sufficiently unique; and
- rules that address certain required matters (such as object, purpose, and meeting procedure etc); and

- one or more members; and
- three or more committee members, at least one of whom must be ordinarily resident in Papua New Guinea; and
- one or more public officers, at least one of whom must be ordinarily resident in Papua New Guinea; and
- a registered office in Papua New Guinea.

Types of incorporated association and annual returns and audit requirements

The new Act will distinguish between two subcategories of incorporated association: the member benefit association and the public benefit association. The former is an association incorporated primarily for the benefit of its members while the latter is an association incorporated for a charitable purpose that benefits the public interest. The classification will turn on the contents of the rules of the association. The practical effect of this distinction will arise in the compliance and reporting obligations of the incorporated association.

In short, an incorporated association must prepare financial statements where; in any accounting period it has an annual gross revenue of an amount greater than the annual gross revenue amount threshold established by Regulations; or receives grants in any amount; or receives donations from the public that exceed the annual donations amount threshold established by the Regulations.

However, where an incorporated association under its rules allows members to benefit, it may opt out of the requirement to prepare financial statements if it can satisfy that the member benefit association did not receive donations from the public that exceed the annual donations amount threshold in the accounting period; or the member benefit association did not receive grants in the accounting period.

Overseas associations carrying on activities in PNG

There are now specific rules relating to overseas associations and the extent that they can carry out their activities in Papua New Guinea. Where an overseas association does carry out activities in the country, it will be required to obtain a certificate of registration under the new Act. Simply carrying out isolated or non-recurring administrative matters is unlikely to qualify an overseas association as carrying out activities in the country. However, failure to register carries a steep penalty of PGK50,000 for each day that the association conducts operations without a certificate of registration.

Transitional rules

The new Act requires existing incorporated associations to reapply for registration with the Registrar of Companies within a year of the commencement of the new Act in order to continue to carry on as an incorporated entity. Failure to do so will result in removal from the register. Associations that are incorporated under the old Act may need to amend their rules if they do not conform with the elements of incorporation in the new Act.

Cybercrime in PNG: What businesses need to know to stay safe

by Happymabel Ketias-Zingunzi, Associate Director, Advisory Services

In our last Kundu newsletter we outlined the risks in particular for Small and Medium Enterprises around cyber security and the move towards outsourcing the cyber function to a Chief Information Security Officer (CISO).

Cyber is very much a live issue for PNG businesses – we are not insulated from the cyber risks that impact other businesses around the world. Cyber is the one area where nothing short of 'best practice' will suffice in order to protect your business as cyber threats are constantly increasing and evolving.

We have set out below some real-life examples of cyber incidents that have impacted PNG businesses.

- In 2022 we were reviewing the IT environment of an audit client as part of the annual financial audit process and as part of this process we found an unknown generic account on the client's network that had been active since 2016. The account was set up through a hacking method called Backdoor. This is when an account is created on the network and automatically sends information to an offshore server without being detected. Backdoors enable hackers to gain command and

control (C&C) of the targeted network without being detected and may use legitimate websites or services to communicate with the offshore server. The frightening thing about this is that the company had no idea their systems were being monitored on an ongoing regular basis by an outside hacker. Information has value and hackers can exploit this value undetected. This is lesson for all businesses – just because you have not received a ransom request this does not mean you have not been hacked and you are not being watched.

- A targeted email with a malicious document attached was sent to a finance staff member within a PNG business. The email was addressed from another team member and on first glance looked legitimate and even replicated a previous internal email. The user reported this email as a phishing email. After analysing the email, it was noted that the hackers had embedded a keylogger virus that was designed to go undetected, meaning it operates silently in the background without raising any suspicion or triggering antivirus software. In this case, it would record the keystrokes of the staff member, allowing the hackers to obtain sensitive information like their password and potentially gain unauthorized access to bank accounts or systems.

- Just this month, a notorious cybercrime syndicate called CI0P has made headlines globally for its ransom demands. The group has also been said to have targeted certain PNG companies. In the past few weeks, the group reportedly obtained confidential data after hacking a third-party software that several companies used to transfer confidential information. Victims are given seven days to pay the ransom demands, or they would expose which companies had been hit and leak the stolen data on the dark web.

These examples highlight the importance of active monitoring of your user access listing both on application and domain level and periodically reconciling it to a staff listing. Without monitoring, you could be breached by hackers who infiltrate your network and remain undetected for extended periods of time. Once inside your network hacker tries to capture elevated permissions that allow the hackers greater control over network resources.

The pattern in PNG is for hackers to look for administrative-level credentials at either local or domain level, allowing them greater control and increased visibility of network resources whilst they remain undetected on the network. Once through the firewall, they will study staff patterns and conduct several activities undetected until they reach their end goal – stealing money or sensitive information or causing long-term damage to your systems and reputation.

Data exfiltration is generally a priority. Once in possession of corporate information hackers can search for sensitive details – like credit card numbers – or sell the data to a third party. Where exfiltration is not possible, criminals will search through databases and applications looking for bank accounts, stock trading accounts, corporate encryption certificates, or anything else they may be able to sell. Although it has not yet been reported in PNG, in recent months worldwide there have been several examples of insider threats causing data breaches in companies. For instance, a former employee of an overseas Medical Center accessed sensitive data without internal obstacles and sent it to their personal emails and started threatening the patients that they would disclose the information. This highlights the importance of implementing best practice around data security and access segregation to prevent data and cybersecurity breaches.

Some of the cybersecurity techniques to help prevent and detect breaches include:

- Monitor network activity for unusual behaviour, such as someone sitting on the network spying and taking data offsite. Do this by regularly reviewing your user listing for all accounts on the application layer database layer as well as network layer.
- Conduct regular cybersecurity training for employees to educate them on data breach risks, attack techniques, and how to ensure reliable data security.
- Identify the computers or servers where sensitive personal information is stored and provide privileged access to these servers on a need-to-use basis.
- Implement access controls, such as multi-factor authentication, to limit access to sensitive data.
- Regularly update software and hardware to ensure that security patches are up to date.

In conclusion, companies in Papua New Guinea should take cybersecurity seriously and implement best practices to protect their sensitive data.

IRC audit activity

As part of their ongoing transfer pricing audit on logging companies IRC announced this week a K140m liability imposed on a multi-national logging company operating in PNG. The announcement illustrates IRC's growing experience in the matter of transfer pricing.

According to the IRC's circular, based on a risk assessment on the taxpayer, the taxpayer had significant volumes of transactions with related parties, did not file Schedule Seven (International Dealing Schedule), was disclosing annual and historical losses in its income tax returns, and had not paid any corporate taxes in PNG for several years. The main transfer pricing issue uncovered by the audit was that the taxpayer sold log species to related parties at prices lower than international market prices and thus reported a lower income than if its logs would have been sold at arm's length.

IRC performed a financial analysis of the taxpayer, considering liquidity, solvency, operational efficiency, net profitability, and working capital indicators, among others. The IRC concluded that the taxpayer's financial performance shows a business that is not sustainable as its liabilities exceed its assets, it is at risk of bankruptcy, its revenues are not enough to cover its costs, it is not in a financial position to commit capital to growth and expansion, and it is financially unable to operate on a day to-day basis. From a transfer pricing perspective, arguments such as these imply a non-arm's length behaviour as it is difficult to understand that an independent business can maintain itself operating in the market with such a poor performance and such negative financial results.

The IRC concluded that the taxpayer was related to the overseas parties based i) on management (same directors managing different entities), ii) on shareholding and common interests (same people holding shares in same entities), and iii) on arrangements that would never take place between independent persons. In addition, the taxpayer's Notes to the Financial Statements listed both companies as related parties.

To determine the arm's length price of the exported logs, the IRC performed a comparable search of log prices for the various species sold by the taxpayer, using a public source of tropical timber prices. Based on it, the IRC calculated the deemed revenues the taxpayer should have realized to reflect market conditions.

What is clear from the above is that IRC are going to great lengths to analyse and prove their cases and their experience in transfer pricing matters is growing.

IRC mapping exercise

IRC have been conducting their door-to-door business mapping exercise in NCD this month. In some cases, the IRC sent the notice in advance, in others they turned up at the door. Generally, the notice letter stated that IRC officers have full and free access to all buildings, computers, documents etc and have the right to seize, retain and remove documents and computers for inspection. Despite the general tone of the letter, in our client's experience thus far, the visits were generally an information gathering exercise whereby the IRC asked the businesses to complete a sheet containing details of company name, address, TIN number, owner names, director names and their contact details.

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

Ces Iewago
Managing Partner
ciewago@kpmg.com.au

Herbert Maguma
Partner
hmaguma@kpmg.com.au

Karen McEntee
Partner
kmcentee@kpmg.com.au

Pieter Steyn
Partner
psteyn@kpmg.com.au