# Let's chat

**Why should cyber risk management be a top priority to family business leaders in Papua New Guinea?**

April 2023

Since early March 2020, business leaders in Papua New Guinea (PNG) have been in solution mode. The main purpose for many family business leaders in PNG between March 2020 and mid 2022 was to keep their businesses open for business and their people employed. During this period business leaders have been reacting to the challenges faced or opportunities presented rather than being proactive. Most of these challenges were due to the shut down of economies and societies during the global pandemic and included: moving to remote work and then back into the office, patching up supply chains, managing cash flow and combating the staff shortages that periods of closed offices or borders have created.

While economies and societies have now opened up, the challenges and opportunities that we have experienced over the past three years are likely to continue to change. Finding smarter, and better, ways to deal with governance issues and managing increasing business and compliance risks will no doubt become a popular agenda item, as decision-makers look to reduce the risk of being blindsided by adverse events.

In particular, cyber risk management has become more of a focus area for businesses, both internationally and domestically. PNG has experienced an increasing number of cyber attack incidents within the private and public sectors. Unfortunately we are observing on a regular basis that there has been another victim of cybercrime.

## What is cybercrime?

Cybercrime covers a wide variety of offences that present a significant threat, including identity crime, computer hacking, phishing, botnet activity, computer-facilitated crime, and cyber intrusion directed at private and national infrastructure and individuals.

**Based on discussions with our clients and other business leaders in PNG, a significant proportion of them have experienced some form of Cyber attack in the past three years.**

pwc

**In PNG, cybercrimes are specifically made illegal under the *CyberCrime Code Act 2016* (the Act). The Act classifies offences into four separate Divisions, as follows:**

| **Division 1**<br>Offences Related to the Integrity of Data and Electronic Systems or Devices | **Division 2**<br>Computer Related Offences | **Division 3**<br>Content Related Offences | **Division 4**<br>Other Offences |
|---|---|---|---|
| • Unauthorised access or hacking<br>• Illegal interception<br>• Data interference<br>• System interference<br>• Data espionage<br>• Illegally remaining | • Electronic fraud<br>• Electronic forgery<br>• Electronic gambling or lottery by a child<br>• Identity theft<br>• Illegal devices | • Pornography<br>• Child pornography<br>• Child online grooming<br>• Animal pornography<br>• Defamatory publication<br>• Cyber bullying<br>• Cyber harassment<br>• Cyber extortion<br>• Unlawful disclosure<br>• Spam | • Cyber attack<br>• Online copyright infringement<br>• Online trade mark infringement<br>• Patent and industrial designs infringement<br>• Unlawful advertising |

Based on discussions with our clients and other business leaders in PNG, a significant proportion of them have experienced some form of Cyber attack in the past three years. Most of these are perpetrated from overseas and the people responsible are unlikely to be caught within the PNG judicial system, but home grown cybercrime is also increasing. For a person to be guilty of a Cyber attack they must, according to section 27 of the Act,

*"intentionally and without lawful excuse or justification, or in excess of a lawful excuse or justification, input or deploy malicious software into an electronic system or device, data, infrastructure, or program resident or transiting within an electronic system or device, for the purpose of altering or causing harm to, or, disrupting, degrading, destroying an electronic system or device, data, infrastructure, or program".*

The worldwide development in information and communication technology has increased dramatically over the past decade. This has provided digital accessibility to a vast number of users in the world. The past few years has also seen PNG begin to catch up on these developments; however, there is still room for improvement. The increased remote working arrangements adopted by many organisations during the COVID-19 pandemic has opened up new threats for cyber attacks as remote access is often left unchecked against current standards, leaving basic security measures neglected. As both the experience of and opportunities for Cybercrime grow it becomes even more important to protect and secure your data.

It should now be mandatory for all employees with IT access to undertake cybersecurity training. Cybersecurity training should be viewed in the same way as other induction or on-the-job training to ensure all staff are fully aware of their roles and responsibilities and the potential risks if something goes wrong.

**As both the experience of and opportunities for Cybercrime grow it becomes even more important to protect and secure your data.**

**As cyberattacks against PNG businesses continue to rise, many business leaders are looking at ways they can improve their organisation's defence against cyberattacks.**

## What is cybersecurity?

There are many definitions of cybersecurity. Even the National Institute of Standards and Technology (**NIST**), which is in charge of defining technical terms used by the US government uses four different definitions of cybersecurity, as follows:

"The prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentications, confidentiality, and nonrepudiation."

"The process of protecting information by preventing, detecting and responding to attacks."

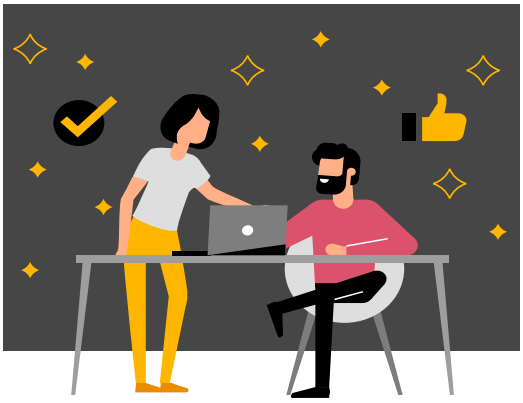
"Ability to protect or defend the use of cyberspace from cyber-attacks."

"[T]he prevention of damage to, unauthorised use of, exploitation of, and – if needed – the restoration of electronic information and communications systems and the information they contain, in order to strengthen the confidentiality, integrity, and availability of these systems".

As cyberattacks against PNG businesses continue to rise, many business leaders are looking at ways they can improve their organisation's defence against cyberattacks. Previous defence mechanisms are proving inadequate, so questions are now being raised about what must be done to increase the chances of success in preventing and responding to cyberattacks.

PwC's 2022 global risk survey identified cyber security as the third biggest risk to revenue growth, behind market risks and business operating model, but ahead of external change and geopolitical risks. At a time when many organisations are reducing their outgoings, spending on cybersecurity may be one of the first areas to be cut back, as it is hard to quantify its benefits. However, perhaps a few examples might help to demonstrate why increased spending in this area is so important.

The 2021 ransomware incident that affected PNG's Finance Department underlined a harsh reality that every organisation must confront - a ransomware attack isn't just a remote possibility, but rather a likely approaching event. Putting organisations under a harsh public spotlight as these events unfold puts incredible pressure on them to pay a ransom as the most expedient mitigating tactic. And ransomware is just one example of many cyberattacks we are starting to hear about in PNG. Unfortunately there was not a lot of information available on all the cyberattacks in PNG (although there was a cyberattack identified by Nasfund Contributors Savings and Loans Society on 1 March 2023 which has been reported in our local media) so we have provided some international data.



The annual *International Crime Report* from the Federal Bureau of Investigation's Internet Crime Complaint Centre (**IC3**) stated that the United States of America experienced an unprecedented increase in cyberattacks and other malicious cyber activity in 2021. Among the top incidents reported were business email compromise and email account compromise which totalled USD2.4 Billion in losses for 2021 (which was up from USD1.8 Billion in 2020).

Victims of cybercrime reported a record number of complaints in the IC3 in 2021 with 847,376. The potential losses for these crimes exceeded USD6.9 Billion. This represented a 7% increase in complaints filed and 64% increase in potential losses.

**Further to this information, here are some recent examples of cyber attacks on organisations in Australia:**

| | | |
|---|---|---|
| Australian unicorn Canva had a data breach in May 2019 that impacted 137 million users. | Optus had a cyberattack in September 2022 that impacted 9.8 million customers. | ProctorU had a data breach in July 2022 that impacted 444,000 people. |
| The Australian National University fell victim to a cyberattack in November 2018 that impacted 200,000 students. | Eastern Health, based in Melbourne, had a data breach which impacted four hospitals. | The Australian Parliament House had political party network breaches in February 2019 which impacted the Liberal, Labour and National political parties. |
| The Northern Territory Government had personal and business email leaked following a breach of its COVID-19 check in app, which impacted 4,400 emails. | The Tasmanian Ambulance Data Breach in January 2021 meant that every resident requested an ambulance between November 2020 and January 2021 had their information leaked. | Service NSW suffered a data breach due to a series of phishing attacks. 47 staff email accounts were impacted leading to 5 million documents (10% contained sensitive information) that impacted 104,000 people. |

## Take Action against Cyber Threats and Speak to an Expert

Much has been written about Cyber Security and most people are aware about using complex passwords, being cautious before inserting unknown USB sticks into a computer and how to behave safely on social networks, although it's still surprising how many of us fall down on these simple measures. The potential threat of an attacker is hidden wherever modern technologies are used. It is important to remember there is no one-size-fits-all approach to cybersecurity, as every business has unique requirements and a different risk appetite, which impacts what should be delivered and how.

PwC supports the delivery of cybersecurity programs designed to meet compliance and risk objectives for many leading organisations internationally. That's why PwC have developed ten key tips to help businesses better consider how to defend against the most common cyber attacks.

| | |
|---|---|
| **1** | Pay attention to the warnings your browser is flashing in your face. |
| **2** | Have a different, unique password for every account. |
| **3** | Keep passwords tough enough to guess that even your partner couldn't figure them out. |
| **4** | Do not click on any links that arrive in an unsolicited email, no matter what. |
| **5** | Keep your business accounts separate from your personal accounts. |
| **6** | Do not rely solely on system password change notifications. |
| **7** | Change your passwords often. |
| **8** | Do not tape your passwords onto your monitor, seriously. If you are struggling to remember your passwords then use a password manager application. |
| **9** | Keep all pertinent security software up to date. |
| **10** | Backup your computer and settings often. |

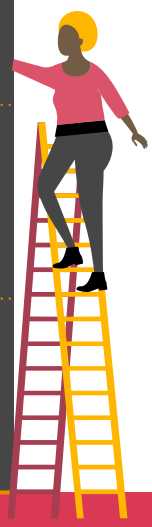
Having the right technology is the starting point. But at the end of the day, being safe from cyber attack comes down to understanding the risks, awareness when on line and individual behaviours. Organisations are only so good as their weakest link. So don't leave things to chance and regret not taking action earlier.

## If you need further information, contact:


**Jonathan Seeto**
Managing Partner
jonathan.seeto@pwc.com

**Michael Collins**
Entrepreneurial and Private Business Partner
michael.j.collins@pwc.com

**Stephen Beach**
Entrepreneurial and Private Business Principal
stephen.beach@pwc.com

**www.pwc.com/pg**