4 POPIA myths you need to know the truth about

https://htxt.co.za/2021/06/4-popia-myths-you-need-to-know-the-truth-about/

30th June 2021

Tomorrow, 1st July 2021, the Protection of Personal Information Act (POPIA) comes into effect in full force and there appears to be something of a mad scramble from local companies to become compliant.

Any organisation that collects, processes, shares or stores personal information about South African citizens, organisations or legal entities must comply with the law and if not, fines or worse could be on the cards.

Unfortunately, POPIA can be rather vague in parts, leaving some to interpret the legislation in ways that could ultimately hurt those heeding that advice.

Thanks to Brian Pinnock, a cybersecurity expert at Mimecast, some of these myths have been debunked and it's vital you and your business aren't caught out by these myths.

Myth #1 – It's only a data breach when data leaves the organisation

This is perhaps the most dangerous myth because, well a data breach implies that data has left the organisation. However, Section 5 of POPIA is clear that a "breach" would also include unauthorised access.

"Mimecast's State of Email Security Report 2021 found that 47 percent of all South African organisations suffered a ransomware attack in the past year," says Pinnock. "This trend is likely to continue when one considers the significant financial rewards for cybercriminals who demand sizeable ransoms from the organisations whose defences they breach."

Myth #2 – I can outsource my compliance

This is a big one and we have heard it uttered more times than we can count since POPI was but a wee bill.

This myth appears to be borne from the idea that the services you make use of also needing to be compliant with POPIA. While it is true that your services need to be POPIA compliant, as Pinnock points out one can't expect compliance to rest on one service provider.

"No one vendor or solution can ensure full POPIA compliance. A vendor – for example Mimecast – can certainly help organisations become compliant to some provisions. There are multiple other moving parts that organisations need to attend to if they are to be fully compliant," the cybersec expert explains.

"It's also not enough to simply take out cyber insurance as a mitigating force, since it provides little to no security against intentional negligence or illegal activities. If the right measures are not in place, it's unlikely the insurer will pay out in the event you fall victim to a cyberattack," adds Pinnock.

To be absolutely clear, it is recommended that you make use of service providers that are POPIA compliant as it does help with compliance. It should not be seen as a silver bullet.

Myth #3 – It's easier to pay a fine than it is to comply

This is a very dangerous myth and the fact that it has been able to spread is jaw-dropping.

In Section 107 of POPIA the penalties for a person convicted of breaching the Act are laid out clearly. Depending on the violation you could find yourself in prison for up to 10 years or a fine could be issued or both.

Some contraventions only carry a maximum of 12 months in prison or a fine but do you really want to find out how far you can push the envelope?

There's also the damage to your organisation's reputation should it be found that it was negligent with user data.

Myth #4 – Any breach puts my organisation at risk of non-compliance

Now for a bit of good news. While one may assume that a breach will result in fines or imprisonment, that isn't the case.

"Under Chapter 3, Section 19 of POPIA, organisations must take appropriate measures to prevent '(a) loss of, damage to or unauthorised destruction of personal information; and (b) unlawful access to or processing of personal information'," says Pinnock.

"The key here is to take 'all reasonable steps' to protect personal data. Organisations can still be considered compliant even if they fall victim to a data breach, provided they can prove that they took every reasonable step to prevent such a breach," he adds.

We feel that this is perhaps the most important part of POPIA as it puts the onus of data protection on those that hold the data and not the user. The hope is that organisations are more careful and put measures in place to prevent intrusion and theft.

POPIA serves as a way to hold organisations who are reckless with user data to account and we hope that this is what the Act does.