What do you do if your business has been hacked?

The recent Experian data breach saw close to 800,000 businesses along with over 24 million South Africans' information left on the internet exposed to cybercriminals. After Experian's earlier announcement that the stolen data had been retrieved and accounted for, the data has surprisingly resurfaced again on the internet, now being shared via a Swedish Company - WeSendit.

Photo by Andri© from Pexels

Questions facing South African businesses are, what harm can come out of this data breach and how businesses can protect themselves?

According to Maeson Maherry, chief executive officer at LAWtrust, “it is unfortunate that once your data is out there, there’s no way of retrieving it. There is a great likelihood of some of the affected businesses having their consumers’ personal information being used by cybercriminals to take part in illegal activities”.

1. Have a recovery plan

The first thing that businesses should do is to consider the importance of having a breach recovery plan. Responding to a breach needs to be both efficient and fast. Having a strong breach recovery plan will always help minimise the damages a data breach can bring for any business.

2. Cybersecurity training

Also, businesses should invest in the latest cybersecurity training for their employees. Routine employee training and education is especially crucial as it ensures that they are informed on the current security and privacy training measures as it will ensure that there are no further data breaches.

3. Monitor data

Maherry states that in light of the various cybersecurity experts’ efforts to prevent a similar incident from occurring,

South African businesses must monitor and track the transfer of data through their systems. This will prevent the data from being misused or exploited.

4. Limit access

He further recommends limiting access of certain individuals among their employees; specifically those not connected to departments, and make sure that sensitive data is handled only by relevant personnel.

5. Stay updated

Often, software that is not up to date and unattended vulnerabilities within business systems make it possible for data breaches to take place. These should always be handled in a timely manner. Furthermore, businesses should never allow or use devices that are not encrypted, as they are more prone and vulnerable to cyber-attacks.

Maherry's final advice to businesses is that they should not wait until they are victims of a data breach. He also emphasizes on the importance of having efficient cybersecurity measures in place. Should businesses be vulnerable, however, their cybersecurity experts will be able to detect the risk and prevent the breach from occurring.