Combatting the rising threat of cybercrime

By John Brown, Head of IT, Fairheads Benefit Services

It is no exaggeration to say that cybercrime is one of the most dangerous and widespread threats to business worldwide. In 2020, more than 51% of all organisations worldwide experienced some form of ransomware attack causing business disruption. On average each organisation experienced three days of downtime.

There are some scary global statistics:

- Cybercrime is expected to inflict a total of $6 trillion USD in damages in 2021
- Global ransomware damage costs are predicted to reach $20 billion by 2021
- The average cost of a data breach is $3.86 million as of 2020
- 86% of breaches in 2020 were financially motivated and 10% were motivated by espionage

South Africa echoes the global trend and is in the unfortunate position of recording the third highest number of cybercrime victims worldwide, with some local stats to back that up:

- R2,2 billion is lost each year to cyberattacks
- 42% of South African Internet users were hit by cybercrime in 2017
- Interestingly, 90% of cybersecurity breaches are due to human error
- Two out of three Malwares are installed via email attachments
- User-downloaded viruses are responsible for 2 two 5 million attacks per day.
- 45% of breaches featured hacking, 17% involved malware and 22% involved phishing.

In 2020, Experian experienced a data breach exposing the personal information of some 24 million customers 793,749 businesses. Thankfully on this occasion the perpetrator was apprehended, and the stolen data was secured and deleted before any damage could be done. More recently, in 2021, Virgin Active experienced a sophisticated cyberattack in which they had to take all their systems offline for days until forensic experts could investigate the incident.

Best practice in combatting cybercrime

Companies should aim to adopt a best practice framework such as Information Security Management System (ISMS). ISMS is a systematic approach to managing sensitive company information including people, processes, and IT systems.

Adopting a multi-layered approach to combatting cybercrime is key. This entails putting in place protective measures at both the front end and the back end of your company's IT systems.

To use the analogy of home security – only too familiar to South Africans - the front end could be a high wall and an electric fence around the perimeter of the property. In IT terms, this could be email advanced protection systems and firewalls.

The back end would be the on-premises protection needed. In a home this would be a burglar alarm, burglar bars and trellis doors. The equivalent in IT systems would be to deploy end-to-end data protection and artificial intelligence (AI) autonomous response systems to protect your on-premises and cloud systems and data.

Wherever possible, data should be encrypted and regular penetration tests conducted. The aim should also be to conform with the best IT governance practice by obtaining, through audits, the international standards of ISO 27001 and ISAE 3402.

Let's hope all South African businesses can up the game when it comes to cybersecurity, so that we can drop down the ranks from being the third most susceptible country worldwide.

ENDS