Security breach puts Liberty at risk – Redstor

While established insurance firm Liberty continues to throw everything it has at an investigation into the recent major data breach, the incident is a stark reminder to businesses that cyber security should be a constant priority – a company's guard must always be up.

This is the warning from global data management Software-as-a-Service specialist Redstor.

While investigations are ongoing, there is speculation that the root cause of the breach was due to a strain of Ransomware which allowed hackers to extract data from systems, the company adds.

Perpetrators have attempted to extort 'compensation' from the organisation and threatened to leak the data.

On Saturday 16 June, Liberty began contacting customers to inform them of the breach stating:

"Liberty regrets to inform you that it has been subjected to unauthorised access to its IT infrastructure, by an external party who requested compensation for it… we have taken immediate steps to secure our computer systems and are investigating the incident"

According to Redstor, some sources claim that the breach came via an email server and that data was extracted from this - but with the alleged dataset stolen, said to be 40 terabytes, it would appear that core systems may have also been accessed.

It has been reported that the Liberty Group's share price dropped 4% in value, following the news of the breach.

"Clients are likely to be worried about how the breach occurred and may lose confidence in the organisation," said Danie Marais, Director of Product Management at Redstor.

"In addition, the organisation will need to establish how the breach occurred, determine the full extent of it and be ready to share this information with regulators. The likely end result will be a fine. The company has stated that they refused to pay the ransom, although CEO David Munro said that he was unable to confirm the amount asked for."

Munro is quoted as saying, "It's fair to say an event like this is not something one can prepare for specifically. We prepare for them generally, but when an event like this takes place, it's out of the blue. This occurred on Thursday evening. It took a couple of days before deciding we should inform customers and ensure that we can safely move into the public domain, as it is a complex matter… We back up our data. The challenge every enterprise has globally is the confrontation from cybercriminals attacking on a regular basis."

Breach threats

Redstor described the Liberty breach as one of many cyber-attacks and ransomware attacks that have affected organisations in recent years.

The company lists South African firm 'ViewFines' as a recent example after they came under scrutiny when data of nearly 1 million citizens leaked including addresses and National Identification numbers.

It added that last year credit agency, Equifax, suffered one of the largest data breaches in history when they lost records pertaining to over 140 million people. This was mainly in the United States but also included data subjects in Europe, the UK and Canada.

Consequences of a data breach

In Europe, the GDPR is new legislation on how organisations and individuals should deal with data protection.

Under the regulation organisations who fail to comply and suffer a data breach are liable of fines up to £17,000,000 or 4% of global turnover. In South Africa, the Protection of Personal Information Act (POPI) is being passed and will be the overriding law.

"Fines are not the only reason for organisations to be concerned with a potential data breach. Increasingly, customers count on an organisations reputation before making buying decisions and companies with bad reputations regarding data security are at risk," Marais added.

Redstor advises that companies should seriously consider implementing best practices around data protection, those that will ensure cyber security is strengthened and that the business is fortified to prevent an attack.

"Cyber-security processes and procedures are vital in ensuring that a breach does not occur. This must include how long data is kept for and the security around how data is stored," Marais continues.

"Sensitive data and data relating to data subjects is what will be targeted by hackers and cyber-criminals. By limiting access to this data, organisations can help to limit the effects that phishing scams may have for those looking to access information with legitimate, but stolen, passwords."

Although widely acknowledged and regularly discussed, the issue of password protection remains a weak point in many businesses' overall cyber security strategy.

Marais explains, "Password attacks are still one of the most common ways that systems are accessed by unauthorised parties.

Botnet attacks in particular, regularly make use of accessing systems, often using default administrator passwords. It is vital to ensure all passwords have been updated and are secure.”

Redstor emphasises that ransomware and other types of cyber-attacks often compromise data, deleting it or making it inaccessible.

“Having a secure off-site copy of all data as a backup will ensure an organisation can recover from an attack and help prevent data loss,” Marais says.

Redstor also advises those who unfortunately do experience a ransomware attack not to pay a ransom.

The company explains that paying a ransom is one way to get data back, but it is not recommended because not only is there no real guarantee that data will be returned correctly, cyber-criminals may strike again knowing that an organisation is vulnerable.

To find out more about how to protect against the threats of cyber-crime, download the latest whitepaper from Redstor here.