BIZCOMMUNITY

The link between insurance and cyber resilience

By Iniel Dreyer

4 Oct 2018

In a landscape where cybercrime is on the rise, insurers and advisors have an added duty of care to protect their clients' data, be it the personal information of a single individual, or the highly sensitive data of a large corporation. So their entire value proposition is dependent on their cyber resilience.

Iniel Dreyer, managing director at Gabsten Technologies

What is cyber resilience?

In a nutshell, cyber resilience is an organisation's ability to withstand – or quickly recover from – any cyber event that may disrupt its ability to operate normally and deliver on client requirements, as usual. It's closely connected to cybersecurity and disaster recovery (DR) – all of which collaborate to ensure business continuity.

Cybersecurity comprises the resources and processes that an organisation leverages to ensure cyber resilience; DR is the organisation's ability to quickly recover from any disaster, whether data loss or natural disaster; and business continuity is a holistic overview of an organisation's ability to continue operations across all functions.

So what does cyber resilience have to do with the Insurance industry?

Insurers and their trusted advisors, need to ensure their cyber environment is resilient against attack, loss of data or any other mechanism which could compromise their ability to protect their client's data. With many insurers breaking out into the field of cyber insurance – insuring their clients against data loss – it's become even more important to have a sound cyber resilience strategy in place, as an example to clients.

How important is it?

We've touched on the importance of cyber resilience as a requirement for maintaining a solid reputation, however, it's also become a requirement for compliance. The insurance industry has always been heavily governed by regulations and there are many standards in place that insurers have to comply with. Today, data specific legislation such as the General Data Protection Regulation (GDPR) has come into effect in the European Union (EU) while the Protection of Personal Information (PoPI) Act) is looming in South Africa. This is making data protection – in the right way – even more critical.

Most large insurance companies have the necessary measures, policies and strategies in place to ensure cyber resilience, however this is a sector that is experiencing rapid growth as new, disruptive players enter the industry. Newer and/or smaller insurers are strongly focused on gaining market share and disrupting the status quo, so cyber resilience may not be given as much consideration as it warrants.

Nonetheless, to compete against the giants, especially with little legacy trust built up, these are exactly the insurers who need to prioritise cyber resilience and make it part of their reputation and value proposition.

What is required?

Quite simply, a generator and a data backup device are just not enough. Sure, a generator is an essential component of cyber resiliency and business continuity, as well as to offer a measure of systems defence against surges, however, it does not ensure cyber resiliency on its own.

A data backup is absolutely critical, as an organisation needs to be able to recover data quickly and reliably in the event of a data breach, cyber-attack or basic loss of data (human error, systems failure, etc.). Conversely, cyber resilience determines an insurer or Advisor’s ability to be resilient against data loss or cyber threats. Therefore, more is needed.

Many organisations aren’t aware of a data breach or loss of data when it occurs. Data can be siphoned out of a business with no one being the wiser until it is eventually detected – often, far too late. A proper data management system that proactively monitors, manages and protects data is a necessity.

Such a system ensures that alerts are sent out not only when there is a breach or loss of data, so that the business can react and respond, but also when there is cause for potential alarm. It proactively scans data activity and can identify anomalies that point to potential weaknesses in the cyber environment, alerting the organisation to attend to them before they become an issue.

It’s also paramount that insurers spread awareness of best cyber practices throughout the organisation, so that all employees – and even clients and suppliers – understand the parameters of data handling, be it their own or another’s. Data and security policies need to be drawn up, communicated and absolutely adhered to, so that - with every person and every bit of data - the risk of attack, loss or damage is reduced.

Well-rounded, solid cyber resiliency is the product of integrated data management systems, data backups, power backups, and the people and policies which work with them, building a reputation that insurers and advisors can, well, take directly to market.

ABOUT THE AUTHOR

Iniel Dreyer is the managing director at Gabsten Technologies