Data protection isn't just an IT issue, says BIL Logistics

According to a report released last month by IBM, the average total cost to an organisation of a data breach is R65,8m.

TheDigitalArtist via Pixabay

The IBM report, namely the *Cost of a Data Breach Report 2020*, surveyed 17 countries including South Africa, with 524 organisations that had experienced data breaches, holding more than 3, 200 interviews with individuals from August 2019 to April 2020.

In South Africa, the average total cost of a breach for this year came in at R36,4m, compared to R52,1m last year, with an average of 228 days (compared to 280 days globally) to identify and contain a breach. "Although data-breach costs may have decreased this year, South Africa is still heavily prone to the issue," says Lesiba Sebola, information technology director for Bidvest International Logistics (BIL).

Supply chain sector reports nearly 300 cybersecurity incidents

Ransomware attacks, which encrypt data and block access to systems until a ransom is paid, have become the most common and costly form of cyberattacks in the supply chain industry.

At the end of 2019 a large US-based firm was hit by a malware attack, in which cybercriminals instal malicious software on the victim's device/s without their knowledge to gain access to personal information, which cost the firm R119,3m in less-than-truckload (LTL) revenue. And in February this year North America's second-largest freight broker (by revenue) was hit by a cyberattack that saw an opening-up of carrier's accounts, tax ID numbers and bank-account numbers.

While the problem has seriously impacted on supply-chain entities, the industry is by no means the only one affected. "There've been a number of reported security incidents, although not specific to the supply-chain sector, that have reverberated throughout the country," says Sebola.

These include

- The hacking of insurance giant Liberty Life's email repository,

- The installation of spyware on transport operator Gautrain that cost the entity R11m,

- A hack into the Civil Aviation Authority's systems,

- A ransomware attack on Tracker, a stolen-vehicle-recovery company, and

- The recent Experian incident which saw as many as 24 million South Africans' personal information put at risk.

"In most of these incidents, the underlying cause was social engineering, which, in the context of data security, is manipulating people into divulging confidential or personal information that may be used for fraudulent purposes," explains Sebola.

Data breaches the challenges of the new industrial revolution
DMASA 25 Aug 2020

The report revealed a growing divide between organisations that have advanced security processes and those with less advanced protocols in these areas. And while many people believe that data protection is an information technology (IT) issue, BIL doesn't hold this view.

"IT is just a component in the protection strategy," notes Sebola. "There's no specific point or phase in a typical supply-chain workflow when data is at its most vulnerable – it needs to be protected throughout. The financial phase may be the most targeted, especially when it comes to payment schedules, but the same can be said for information regarding expensive cargo being shipped, so throughout the process data needs to be closely guarded.

> “ *Companies need to get the basics right as far as developing and implementing a cybersecurity policy, and then to adhere to it.* ”

"Every employee is a developer of data: they're the first custodian of data that they've developed, so the responsibility lies with them on how to share and store whatever it is they've generated or received. Our industry is undergoing rapid digitisation, which means that data is increasingly being shared and stored by third parties like suppliers, vendors and other business partners, so the need to protect it couldn't be greater."

BIL, for example, developed a cybersecurity policy which includes controls such as employee conduct while utilising the company's network, installing and running security programs, and ongoing security maintenance. The policy also maps out the roles and responsibilities for all employees pertaining to the issue, regardless of their role or level of seniority.

Sebola says that IT department's should provide the necessary technology to ensure that this is upheld. And ideally, a data information officer, as prescribed by the Protection of Personal Information (POPI) Act, is ultimately the custodian of data protection within an organisation. He/she would develop a data governance framework that entails how the data is handled within the organisation.

Impact on industries

As the exchange of data rapidly gathers pace around the world, several industries reliant on the global supply-chain market are at increasing risk of coming under cyberattack.

Healthcare, energy, financial services and pharmaceuticals experienced an average total cost of a data breach significantly higher than less regulated industries such as hospitality, media and research, according to the IBM report. Global data-breach costs in the healthcare sector increased by 10,5%, with energy increasing by 14,1% to R108,9m, and retail by 9.2% to R34,2m.

The study also found that many organisations believed remote work during Covid-19 would likely increase data-breach costs, as well as the time required to identity and contain a breach. The study found that having a remote workforce would increase the average total cost of a data breach of R65,8m by nearly R2,3 million for an adjusted total cost of R68,1m.

But, Sebola says: "There’s light at the end of the tunnel in all of this. Companies need to get the basics right as far as developing and implementing a cybersecurity policy, and then to adhere to it."

Fundamentals should include:

- Providing a new and continuous awareness programme for employees,

- Conducting top-to-bottom security audits,

- Keeping software and systems current and updated,

- Performing regular data backups, and

- Implementing a layered security environment.