The consequential implications following a Data Breach and the Mitigation of same

Kristi Erasmus

14 October 2019

Source - https://www.tech4law.co.za/tech-advisor/security-d91/the-consequential-implications-following-a-data-breach-and-the-mitigation-of-same/

The consequences of a cyber-attack or its related data breach are wide and far reaching, impacting customer trust in the organisation and its ability to safeguard personal information, eroding an organisations ability to retain existing customers or attract potential future customers and additionally exposes the organisation to more risks, including but not limited too: business interruptions, disclosure of sensitive or personal company information or processes, reputational damage and regulatory investigations and fines. (Ramotsho, 2018)

The cost implications and loss of a data breach often lingers for some time after the initial data breach, with only an average of 67% of the costs of a data breach being experienced in the first year after the breach, with 22% of the costs being felt in the second year and 11% of the costs occurring more than 2 years after the initial breach of data. Organisations in highly regulated environments such as financial institutions and law firms experience an even longer trajectory of data breach costs, with 53% of costs experienced in the first year after the breach, 31% thereafter and as much as 16% more than two years after the breach. (Ponemon Institute & IBM Security , 2019)

The costs of a data breach and the reputational damage and consequential financial implications of a cyber attack can be significantly mitigated where a proper plan of action has been prepared and is ready for implementation following the discovery, identification and detention of the data breach. To adequately prepare and plan a response to a data breach or cyber attack an organisation should start by determining its risk of exposure by firstly considering the organisations regulatory compliance market, secondly determining the business assets or data assets that are critical to the business, thirdly determining the likely threats to an organisation including but not limited to previous, disgruntled employees, external hackers, criminal or system vulnerabilities and lastly to not only ensure focus and security for electronic data and records but to ensure the same security standards and features for paper documents and records. (Ramotsho, 2018)

The cost of data breaches can be significantly reduced where an organisation has an incident response team with a detailed cyber incident playbook which is routinely tested through tabletop exercises or a stimulated breach scenario, providing a detailed plan on how the

organisation will respond to a cyber attack or data breach. (Ponemon Institute & IBM Security , 2019)

Research has additionally indicated that the overall costs of a data breach can be reduced where the organisation has a senior level leader, such as a privacy officer or chief information officer, who reduces customer turnover by enhancing customer trust in the organisations ability to keep and protect their personal information and data, limiting the number of customers that lose trust in the organisation and take their business elsewhere. Additionally, it has been found that an organisation that provides Victim Identity Protection following a breach can significantly reduce customer turnover. (Ponemon Institute & IBM Security , 2019)

Data Classification schemas and retention programmes also go a long way in reducing the costs of a data breach by highlighting sensitive and confidential information that could be vulnerable to a breach and provide ways by which the volume of such information can be reduced. Vulnerability scanning may also significantly assist an organisation to identify database vulnerability exposures and misconfigurations, with the most sensitive information being obscured and encrypted.

An organisations ability to detect and contain damage potentially arising from data breach can be significantly enhanced by security automation and intelligent orchestration capabilities across the organisation's security operations that enhance visibility and detection of breaches. Additionally, an internal framework for satisfying governance requirements, evaluating enterprise risk and ensuring governance compliance will further improve an organisations ability to detect and escalate a data breach

The 2019 global average cost of a data breach amounted to R54 million, with the average data breach size comprising of 25,575 records, which represents a 1.5% increase from 2018. South Africa is not immune to cyber attacks and data breaches, with the 2019 average South African cost of a data breach amounting to approximately R46 million, with well-known South African data breaches including companies such as Liberty Life, ViewFines, Deeds Office, Ster-Kinekor, Standard Bank of South Africa and the SABC, to mention but a few.

Given advancements and improvements in hacking techniques, tools and abilities, the chance of an organization experiencing a data breach within the next two years have increased significantly from 2014. In 2014 organisations had a 22.6% chance of suffering a cyber-attack within a two-year period, which has increased to 29.6% in 2019, reflecting an increase of 7%. Thus, there is a one in three chance of an organisation experiencing a breach within two years.

It is clear that Cyber-attacks and data breaches are a reality of today's 21st century business tools and platforms, demanding the incorporation of highly effective and efficient cybersecurity checks and procedures.