gulfnews.com

Avoiding the pitfalls of a corporate data breach

Organisations in the technology and retail sector are far more likely to have a breach

By Naushad K Cherrayil Staff Reporter
Published: 21:31 July 3, 2014

GULF NEWS

Dubai

Data breaches and stolen information have become a common word across the globe and it is growing every year at an enormous pace.

The latest “Cost of Data Breach Study” commissioned by IBM and conducted by the Ponemon Institute found that the average cost of a global data breach actually increased 15 per cent last year.

“Perhaps even more surprising is that the average cost of these incidences reached an astounding $3.5 million; far more than what many companies consider when evaluating cybersecurity threats,” said Dr Tamer Aboualy, Chief Technology Officer of Security Services at IBM MEA.

He said organisations surveyed in the Middle East region were pretty close to the global median with the average total cost of $3.11 million.

The average per capita cost of data breach in the UAE and Saudi Arabia stood at $108.52.

The maximum data breach cost among the Middle East companies was $12.35 million and the minimum data breach was $400,000.

While some of these are direct costs, the report also identified something called “lost business”; a fact that many organisations forget to account for. This includes the abnormal turnover of customers, having to increase customer acquisition activities, and reputational losses.

“Among the Middle East companies surveyed, we actually found that ‘lost business’ on average accounted for nearly half the total cost of all data breaches over the long term,” Aboualy said.

Criminal misuse

Within the Middle East for example, 50 per cent of the reported incidents involved data theft or criminal misuse as opposed to a system glitch or employee error globally. This is actually a higher percentage than the global average, and this category of incidents also happens to be the most costly type of data breach.

Such recognition may seem simple, but Aboualy said that they are tremendously important in guiding companies to adopt the right kind of external and internal security policies. The study further revealed that certain industries may be impacted more than others. In the Middle East, organisations in the technology and retail field were for instance, far more likely to incur a data breach in contrast to energy and industrial companies. He said that about half of the companies we surveyed globally were found to have

low or no confidence that they are making the right investments in people, process and technologies to address potential and actual threats. Only 38 per cent of the organisations surveyed globally reported to even have a security strategy to protect their IT infrastructure.

Incident response plan

Within the Middle East, IBM found that the most profitable security investments include having an incident response plan, understanding your environment (data classification, access rights and environment risks), and also the appointment of an information security leader with a clear responsibility for breach containment.

On average, Aboualy said that companies would ideally like to invest $14 million over the next 12 months to execute their organisation’s security strategy. Regrettably, in the same 12-month period these companies anticipate having only about half that amount to invest.

He said cyber threats have clearly grown in both volume and complexity over the past few years, with the brash sophistication of recent attacks elevating the conversation from the IT room into the boardroom. Despite the business value of this critical enterprise data, it seems as though “more needs to be done” to help organisations recognise what their “most signification information is, where it resides, and how it can be protected,” he said.