BIZCOMMUNITY

A data breach can lead to job loss

When a data breach strikes, the damage can reach further than a business's finances, reputation, and customer privacy. A breach can also severely impact the careers of individuals at the company involved.

According to a new report from Kaspersky Lab and B2B International, 25% of data breaches in the Middle East, Turkey and Africa (META) region in the past year have led to people losing their jobs.

Breaking careers with data breaches

A data breach in a company can be a life-changing experience for both its customers and employees, according to the recent report from B2B International and Kaspersky Lab 'From data boom to data doom: the risks and rewards of protecting personal data'.

The study shows that 45% of businesses in the META region had at least one data breach in the last year. As for the staff involved, they don't always - not even C-level - get to keep their jobs afterwards.

Suffer a data breach and lose up to one third of your customers
30 Aug 2018

The range of employees laid off after a data breach demonstrates that the incident can affect anyone, and 2017 alone saw a wide variety of people fired as a result of data breaches: from CEOs to a regular employee exposing the company customer data.

Of course, for businesses this means more than just lost 'talent': 43% of META companies have had to pay compensation to the customers affected, over a third (35%) have reported problems attracting new customers, and over a third (36%) have had to pay penalties and fines.

Data beyond control adds to the risk

In modern business, storing sensitive personal data is practically unavoidable: 88% of businesses in the META region and 81% of businesses in South Africa collect and store their customers' personally identifiable information. Moreover, in today's increasingly complex environment, new regulations like GDPR mean that storing personal information comes with compliance risks too.

Is your network ready for GDPR and PoPI?

Bryan Hamman 7 Jun 2018

What makes these risks even more tangible is the actual reality of how businesses store data: approximately 13% of sensitive customer and corporate data in South Africa resides outside the corporate perimeter: in public cloud, BYOD devices and in SaaS applications, which makes controlling the data flow and keeping it safe a challenge for businesses.

Data protection measures beyond policies

The report says that 91% of businesses in the META region have at least some form of data security and compliance policy in place. However, a privacy policy itself isn't a guarantee that data will, in fact, be handled properly.

There's a need for security solutions that can protect data across the whole infrastructure – including cloud, devices, applications and more. Cybersecurity awareness among IT staff and beyond also needs to be improved, as more and more business units are now working with data, and thus need to understand how to keep it safe.

"While a data breach is devastating to a business as a whole, it can also have a very personal impact on people's lives — whether they are customers or failed employees – so this is a reminder that cybersecurity has real-life implications and is, in fact, everyone's concern. With data now traveling on devices and via the cloud, and with regulations like GDPR becoming enforceable, it's vital that businesses pay even closer attention to their data protection strategies," says Dmitry Aleshin, vice-president for product marketing, Kaspersky Lab.