BIZCOMMUNITY

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

Findings from RSA's recent survey in the UK showed that 28% of customers have elected to boycott companies that have been shown to mishandle personal data.

RSA is a global cybersecurity company with consulting and technology solutions that empower firms by providing a holistic view of cybersecurity needs in order to reduce risk and rapidly respond to incidents.

“South African businesses should be prepared for similar consumer trends in the near future,” believes Anton Jacobsz, managing director at Networks Unlimited Africa, which delivers the full range of RSA solutions to the local market.

> *“Consumers are becoming increasingly aware and sensitive about howtheir service providers use their personal data, and for those organisations that suffer high-profile data breaches, there is a very real possibility that customers will ‘vote with their feet’.”*

The survey goes on to reveal that the majority of consumers (57%) have no idea how many times their personal data may have been placed at risk, given the flood of headline-grabbing cyber-security breaches over recent months.

GDPR and PoPI

While analysts estimate that only about a tenth of all breaches is reported to the public, this is about to change, as the European Union’s General Data Protection Regulations (GDPR) finally kicked in on 25 May.

“For businesses operating in the EU, or even for local businesses that provide services to EU citizens, the new laws will ensure that any and all data breaches are disclosed within a 72-hour period,” explains Jacobsz.

Is your network ready for GDPR and PoPI?

Bryan Hamman 7 Jun 2018

GDPR is enshrined in European Union law, giving it automatic credence among all member states. It seeks to harmonise data protection regulations throughout the region, placing stringent rules on how organisations gather and use individuals’ personal data, increasing levels of transparency, giving individuals greater control over how their data is used, and ensuring mandatory disclosure of any breaches.

Under GDPR, companies could face fines of up to €20m, or 4% of annual turnover, which shows the gravity of the issue for large businesses in particular.

In South Africa, the pending arrival of our own incoming legislation, the Protection of Personal Information Act (POPIA), expresses a very similar intent to GDPR. Many legal experts believe that achieving compliance with GDPR should essentially imply compliance with PoPIA, once it is enacted.

Staying on the right side of the law

So just how can organisations set about ensuring compliance with both PoPI and GDPR?

“As a global company, RSA has completed a considerable effort to ensure that it prepares organisations for GDPR - identifying gaps, improving readiness, evaluating risk, meeting compliance and rapidly respond to incidents,” says Jacobsz.

“To cater for such broad-reaching compliance requirements, organisations must address cyber-security and data protection at an overall enterprise level,” he adds.

“RSA’s approach incorporates both advisory and technology services, addressing the entire lifecycle of solution fulfilment - from strategy and design, to deployment and operations management.”

While organisations must comply with new legislation, they also cannot halt progress on key digital programmes and transformation projects. To ensure that their digitisation journeys can proceed safely, RSA takes a business-focused approach to one’s cyber-security strategy, ensuring it is aligned with the company’s strategic objectives.

7 practices to ensure comprehensive defences

In a recent white paper, RSA details the seven key practice areas that it has established to provide comprehensive threat mitigation and ensure regulatory compliance:

1. Risk management

Tailoring global best-practices to the unique elements required for the foundation of a firm's holistic risk management programme, including various assessments and stakeholder mapping exercises.

2. Identity assurance

With identity management at the core of all security programmes (and representing the biggest threat vector), it's critical to design iron-clad identity management policies and technologies.

3. Advanced cyber-defence practice

Identifying gaps, prioritising risks and designing programmes to improve defences, integrate solutions, provide deep visibility, detect advanced threats and reduce mitigation time.

4. Incident response practice

By combining early detection and rapid response, organisations can close the gap between an initial breach and an attacker being able to carry out their objectives.

5. Professional services

The technology deployment expertise to ensure that organisations gain maximum value from their investments in RSA technology sets.

6. Research

With a heavy emphasis on R&D, the security solutions from RSA continually adapt to the ever-changing threat landscape and keep pace with new legislation (such as GDPR), while training services help customers to enhance overall awareness and optimise their cybersecurity capabilities.

7. Enterprise-wide security programme management

To pull it all together, teams of cybersecurity experts analyse an organisation's overall threat posture, continually making recommendations to further strengthen one's security practice.

"The risks of data breaches - for both local and international companies - are enormous," summarises Jacobsz, "ruining an organisation's reputation, destroying customer trust, and exposing them to heavy regulatory penalties."