Five important things to remember about GDPR

With the large quantities of personal data financial services providers handle, they have had their hands full preparing for the Protection of Personal Information Act (PoPI). But there's another piece of compliance legislation that will come into effect much sooner -the European Union's General Data Protection Regulation (GDPR) - and for many, this isn't even on the radar.

Nick Saunders, cyber resilience expert, Mimecast Africa and Middle East

Gartner's report, *GDPR Clarity: 19 Frequently Asked Questions Answered*, predicts that by 25 May 2018, when the legal framework goes live, less than 50% of all organisations impacted by it will be fully compliant.

Unprepared

This prediction doesn't seem to be too far from the truth, especially locally. Despite GDPR being a month away from full implementation, some South African business still remain unprepared that they may need to comply with this piece of legislation if they do business with EU citizens or companies.

A 2017 study showed that as many as 89% of surveyed South African organisations had both personal and sensitive data contained in their e-mail systems. They therefore need to review and retool their handling of this data to ensure it is adequately protected.

Hefty fines

Recently, the Mimecast Email Security Risk Assessment (Esra) showed that the current e-mail security systems of most organisations, are failing to detect and act on thousands of attacks. With GDPR in effect, the exposure of personal information for any EU clients means a hefty fine with the potential to cripple an organisation, if not destroy it.

Legislation has outlined penalties for GDPR non-compliance as upwards of €20m, or 4% of the organisation's yearly revenue, whichever is higher. Businesses who fall victim to cybercrime in the age of GDPR will not only have to deal with the fallout of a successfully executed attack, but severe financial punishments as well.

Five important things to keep in mind regarding GDPR compliance:

1. **Breaches must be reported**

   Currently, if a data breach occurs, an organisation will do its best to cover it, and, depending on the severity, keep it within the confines of the IT department. However, when GDPR is enacted, all hacks that compromise personal data of EU citizens must be reported to the supervisory authority within three days.

2. **Client consent is a must**

   Gone are the days of automatic opt-in. Moving forward, organisations need to make their clients aware of what personal data is being collected, for what purpose and what this information can potentially be used for. This includes their name, address, ID or passport number and more.

3. **The right to data privacy**

   Under GDPR, individuals can request access to, and choose to remove, their personal data from an organisation. They essentially have the right to be forgotten when there is no valid justification for a company to store their sensitive information. Unfortunately, according to the Vanson Bourne study, only 25% of surveyed organisations believed they could retrieve personal or sensitive personal data immediately, with six being the average number of hours businesses would take to recover information.

4. **Data needs to be encrypted**

   Under GDPR, client credentials need to be protected through sophisticated encryption, at both the transit and rest (archiving) stage. At the same time, client data should be easy to retrieve and treat as per the owner's wishes.

5. **Accountability from all parties**

   As IT and other services are sometimes outsourced, client data may pass to external vendors, where it too can be compromised if that particular supplier suffers a ransomware attack. These third parties need to take responsibility and ensure they protect the sensitive information they handle.
   All this said, even if an organisation has the best intentions and does their utmost to protect their clients' personal data, it only takes one unsuspecting employee clicking on a seemingly harmless e-mail for a data breach to occur.

Finally, GDPR may not be relevant to South African businesses that don't employ EU citizens or conduct business in the region, but it is still important for them to consider the requirements for maintaining data privacy as outlined by this regulation. PoPI will soon be enforced and other legislation may become more prevalent across all regions. As a South African business, it's worth building for the future today, rather than waiting until it's too late.

ABOUT THE AUTHOR

Nick Saunders, cyber resilience expert, Mmecast Africa and Mddle East