Protecting 'digital gold' aka Data

October 2020

Data is perceived as good as gold in the digital world we live in today and protecting the data need efforts and investment. There have been several privacy legislations enacted in last few years to protect personal information, Protection of Personal Information (POPIA) is the recent one that has been put in effect in South Africa. These regulations prescribe lawful use of data collected by businesses and provide specific rights to data-subjects (to which the data relates), such as right of access/deletion/objection, to avoid misuse of the information.

Non-compliances to the regulation often results in heavy penalties and loss of reputation. According to GDPR Enforcement Tracker website, there have been 381 reported instances of imposing fines and penalties as high as €50 million. Most of these instances are attributed to ***"insufficient legal basis for data processing."*** There are other instance of seeking higher penalties. According to one instance posted on the Information Commissioner (ICO), UK website "*following an extensive investigation the ICO has issued a notice of its intention to fine British Airways £183.39M for infringements of the General Data Protection Regulation (GDPR)*". With these regulations in place, protecting personal data is often considered more of a liability than an asset and adds to the cost the doing business.

During a conversation with a client (and a very close friend) we deliberated on the reasons for such increased instances of data breach, especially when the businesses are putting more effort and money on data security. While he believed that protecting information in a business environment is easier said than done, my argument was that organisations often overcomplicate such programs, making it difficult to achieve the intended results.

As such, there are not more than a combination of a handful of causes which, if correctly managed, would increase the effectiveness these programs, prevent a breach and optimise the costs of protecting data (which includes personal information).

The following is the superset of these causes…which ones stand out to you as being the most relevant?

1. ***Protect infrastructure for information:*** organisations often make substantial investments in protecting networks, data storages and applications without focussing on information. While it is critical that devices and applications remain protected, the sensitive information is often shared (or stored) outside the controlled environment where the chances of breach are higher. Protecting infrastructure without the sight of information that needs to be protected leads to wasteful expenditure.

2. ***Over-planning and under-preparedness:*** While organisations make substantial efforts and investments in strengthening their cyber defence, many fail to prepare to respond in the event of a cyber-attack. No organisation is outside the target list of cyber criminals and all of us face number of intrusion attempts on our networks. While most of these are blocked, the threat of them being successful is extremely high as there is no impenetrable defence (at least I have not seen one). It is equally important, if not more, to be prepared for an effective response to a data breach.

3. ***Tone at the top:*** Executives are often given more exceptions on security policies and configurations than other employees. Exceptions to security procedures, trainings and insecure configurations on their devices are common practices across organisations. Senior personnel with weaker controls are also better targets for cyber attackers.

4. ***Over-emphasis on technology than psychology:*** Technology is considered a silver bullet. As the majority of organisations' efforts focus on technology controls they miss giving attention to employee psychology. "Security first" and "privacy by design" (and other similar mumbo-jumbos) can only be effective if practiced by human resources and is embedded in the culture.

5. ***Fight algorithms with intellect:*** While the attackers out there work on modern digital technologies, organisations are often conservative in leveraging Artificial Intelligence (AI), machine learning (ML) and other modern technologies to defend, detect and respond to cyber attacks. Cyber-attacks are often dealt best with adequate technology arsenal (without discounting human resilience as mentioned in previous point).

6. ***Protect assets for identity:*** Organisations make substantial investments to protect internal devices, applications and networks but often miss protecting their digital identities. Social media identity of the organisation is often misused and abused by attackers. Thousands of communications are being sent each day, 'impersonating' the brand, with embedded malware. Dedicated efforts are required to monitor social media identity of the brand and take-down the fake identities.

7. ***Late to react:*** While in most cases, the breach happens in few seconds, attackers spend months in reconnaissance and planning. Putting up the right controls for capturing and comprehending early warning signals and preparing for an appropriate response can be game-changer!

KPMG can assist you…

KPMG's multi-disciplinary team of specialists in data privacy, cyber security and technology assurance can support you in preventing, preparing for and responding to data breaches. Some of the services we provide include:

- **Cyber Defence –** Our ethical hacking specialists will help you find your organisation's vulnerabilities against potential breach.
- **Incident Response –** We can help you prepare for data breaches and respond effectively when they occur through our global network of incident response
- **Cyber Strategy and Governance –** Our team of privacy specialist help assessing the current privacy controls and define the the right strategy for enhancing the technology and process controls.
- **Cyber Transformation –** Our implementation team can help implementing data management or governance technologies in your current environment.

Contact our Privacy Team:

Sharmlin Moodley
Partner and member of the KPMG Privacy Team
M: +27 60 992 4789
E: sharmlin.moodley@kpmg.co.za

Rupesh Vashist (author)
Associate Director and member of the KPMG Privacy Team
M: +27 66 101 6590
E: rupesh.vashist@kpmg.co.za

Marcelo Vieira
Associate Director and member of the KPMG privacy Team
M: +27 82 718 8485
E: marcelo.vieira@kpmg.co.za

Beulah Simpson
Legal Manager and member of the KPMG privacy Team
M: +27 60 602 3066
E: beulah.simpson@kpmg.co.za

Finn Elliot
Associate Director and member of the KPMG Privacy Team
M: +27 79 039 9367
E: finn.elliot@kpmg.co.za

dataprivacy@kpmg.co.za

Click here to visit our privacy website