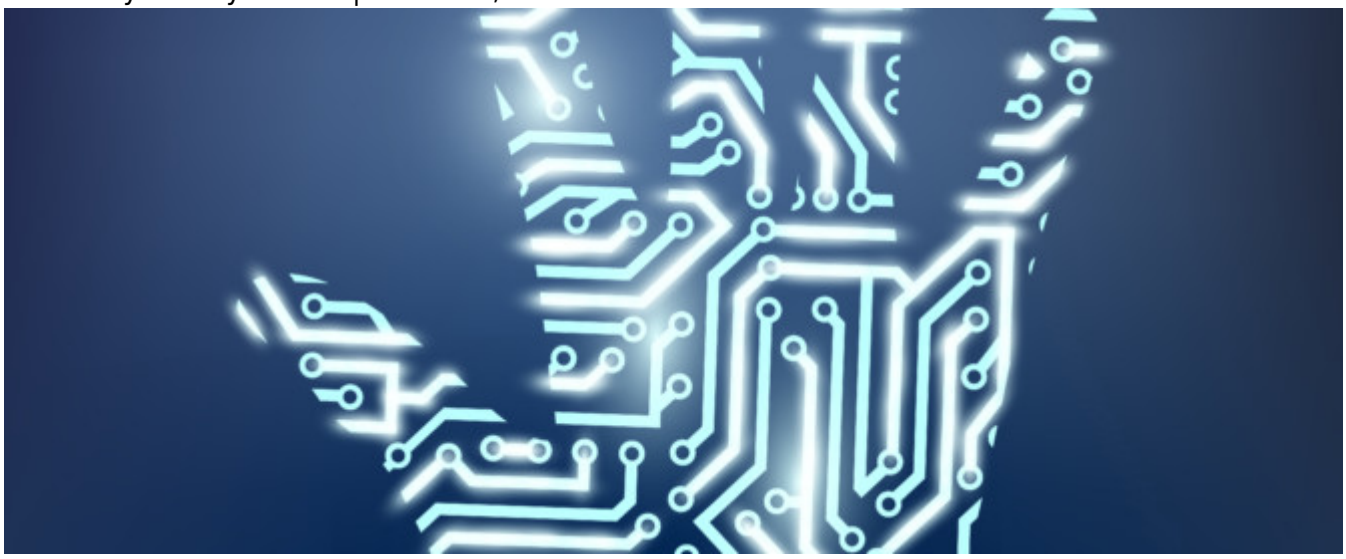
THE INTERNET OF THINGS AND CYBERSECURITY

Category: Commercial Law,Privacy Law, Infosec, and POPIA
written by Melody Musoni | March 20, 2019



We live in extremely exciting yet precarious times. Technological advancements have made it possible for normal objects and gadgets to be equipped with the ability to identify, sense and process information as well as networking and communicating with other devices to achieve some useful objective.[i] This networking of devices to the internet has been termed the Internet of Things (IoT). The Internet of Things has reshaped the way people communicate[ii], do business[iii], participate in politics[iv], obtain healthcare services[v] and has significantly contributed to the economic growth.

Smart devices

Take a wrist watch as an example, it is no longer only for purposes of time keeping but rather has become so sophisticated that it can show your health statistics, your geo-location, the number of kilometers you have walked and if you have been dormant for a while.[vi] If you have interconnected your watch to your smart phone, you can receive your health statistics straight to your email. If your smart watch is connected to your smart home, your smart home can quickly adjust the temperature settings the moment that it picks the signal from your smart watch on your way home. Since your smart phone is interconnected to your home, you won't need to carry around a batch of keys but simply enter a code on your phone which unlocks your home.

Report from the Institute of Risk Management of South Africa

As exciting as all this interconnectivity and the Internet of Things is, the level of risk and vulnerability of people's data and communication networks has also scaled up. The 2019 Risk Report published by the Institute of Risk Management[vii] indicated that cyberattacks are a high risk in South Africa and currently sitting at number 9 out of 20 of the most risky sectors and activities in the country. The report identified that the global dependence on technology, the increasing interconnectedness and accessibility and the growing base of global threat actors, cyber-criminal syndicates are some of the risk causes of cyberattacks.[viii] The report further indicated that the likelihood of cyberattacks happening is very high.

What are the dangers of IoTs

Imagine what will happen if a tech-savvy criminal gets hold of your smart phone? Your smart phone is usually a treasure trove of unlimited information which can get anyone access to your banking details and depending with a criminal's level of sophistication, they can siphon money out of your bank accounts. Your smart phone has details about where your children attend school, their timetables and your calendar and diary which means that a criminal can potentially use that information stalk your family and possibly kidnap your children. The nightmare does not end there, through your smart devices, a criminal can access your linked work emails and unlawfully collect any confidential and sensitive information he or she can lay their hands on. The convergence of the Internet of Things means that a criminal only needs one point of entry either through your smart phone or smart watch and gain access into a whole connected computer network system. IoTs thus pose security threats on data and information systems.[ix]

What can you do?

Do I mean to scare you off from joining the digital revolution and information superhighway? Absolutely not! Anyone who does will be fighting a lost battle as the internet is rapidly becoming indispensable in our lives and it will be a matter of time before everything is completely digitized. There are many basic and yet effective cybersecurity tips that any person who has a mobile phone, email or social media account need to know and implement.

1. One should take all the precautionary and preventative steps to secure their online activities and networks. Gone are the days when you used one password (usually a common word probably your favorite animal or food) for all your accounts. It is crucially important that you have **different passwords for different accounts**.
2. I know most people enjoy the convenience of having their phones or computers to automatically sign them into their accounts, but this also is very dangerous. Always **regularly change your passwords and passkeys** from time to time.
3. A password must not be an easy word but should have **unique characters** like the percentage sign (%) or the exclamation mark (!) and consist of numbers.
4. For businesses, there is need to develop and **implement appropriate safeguards** to ensure that information systems and IT systems are protected.
5. Every business should develop and implement appropriate activities to maintain **plans for resilience** against cyberattacks.
6. IoTs mean that an employee's personal email can be used as a gateway for an attack of a business network. Businesses therefore need to equip employees with cybersecurity skills as well as increasing awareness amongst the employees on the importance of adopting cybersecurity measures.

Adopting these measures is not a guarantee that your information systems and networks will be immune from cyberattacks and cybercriminals, but it certainly fortifies your computer networks and aids in making your networks less susceptible to cyberattacks.

[i] A Whitmore, A Agarwal & LD Xu 'The Internet of Things–A Survey of Topics and Trends' (2015) 17 Information Systems Frontiers; New York 261.

[ii] Information and Communication Technologies and Social Media and Social Networking Platforms allow for real time communication amongst unlimited participants regardless of geographical locations. Facebook, Twitter, Instagram, Telegram, Whatsapp, Facetime, to mention but a few.

[iii] Electronic commerce allows people to purchase products at the click of the button, different mobile apps allow people to do business from ordering food on Mr D App, getting transport using the Uber App etc.

[iv] Social media platforms allow for people to share political ideas, participate in political debates and keep informed of any political developments. Agora also makes use of the internet technologies to allow for citizen voting.

[v] E-health and mobile healthcare services are increasingly becoming popular. Instead of visiting a doctor, patients are able to get medical assistance via mobile apps. Drones are being deployed to areas that are less reachable to deploy healthcare supplies to patients.

[vi] https://www.fitbit.com/eu/ionic accessed 12 March 2019. R Peppet, 'Regulating the Internet of Things: First Steps toward Managing Discrimination, Privacy, Security and Consent' (2014) 93 Texas Law Review 85.

[vii] IRMSA Risk Report 2019 5th Edition. https://www.irmsa.org.za/page/2019_Risk_Report accessed 12 March 2019.

[viii]IRMSA Risk Report 2019 page 63.

[ix] The rising use and reliance on online government and commercial services and the ubiquity of social networks and the emergence of the IoTs all poses security threats on data. Ewan Sutherland "Governance on cybersecurity – The case of South Africa" 2017 (20) The African Journal of Information and Communication (AJIC) 83 – 112 at 84.