Security? - It's Academic!

Senior IEEE member and professor of Cybersecurity at Ulster University, Dr **Kevin Curran**, has warns that IoT will not reach its potential until fundamental security concerns are addressed. At the same time Curran says those who are fined under new GDPR rules will likely be clearly in contravention of the spirit of GDPR.

The Internet of Things has promised to bring numerous benefits to both businesses and consumers for a number of years. From improving efficiency in the workplace to making life easier at home, for IoT seemingly the sky is the limit.

In a year of constant security threats and cyber-attacks against major corporations, Dr Kevin Curran, Professor of Cybersecurity at Ulster University says the security of IoT devices remains a major challenge.

"Compromised IoT devices have been responsible for many large-scale botnets in recent times and this will only hinder the reputation of IoT and slow public adoption and acceptance. Security standards are a key requirement that need to be focused on before implementing for mass adoption in modern life and more accountability for manufacturers with regards roadmaps for updates for any devices they sell."

Curran also advised that data needed as much protection as the devices themselves considering the mass cybersecurity breaches of recent years and the new GDPR rules.

"Companies will have to pay more attention to the secure storage of data collected via the Internet of Things as legal repercussions arrive in the form of the EU GDPR. IoT data is generally stored in the cloud, therefore all the recommended practices applicable to securing data in the cloud equally applies here. Companies – in particular those with large data sets due to the multi-tenant nature of a cloud platform – should pay extra attention to the data lifecycle phases and ensure that aspects such as data destruction is provided as part of the service."

Curran predicts that 2018 will see a corporation hit with a major fine with authorities wanting to prove that the new regulations are not to be taken lightly.

Dr Kevin Curran

"The key to GDPR's effectiveness is of course adherence and adherence will only come about through the hefty fines, which are up to £20M or 4% of global revenue. No one can really say for sure at this stage whether we will see the giant conglomerates suffer such consequences but the EU must bare its teeth sometime to ensure companies do not become lax about the law.

I expect to see large fines. Those who are fined however will likely be clearly in contravention of the spirit of GDPR. Companies who unwillingly breach the rules (even if not a defence) will not suffer as large a fine as those who try to contravene the GDPR spirit in a sly manner. The spirt of GDPR is that any data collected on us should be protected, accurate, available to us to collect, move, delete, modify and see and that they should only collect what is necessary. In other words, do not capture too much and do not treat it lightly."

Dr Curran had more positive news for customers, predicting that the new regulations would result in improved security measures for customer data:

"Cyber security will improve because companies are forced to pay more attention to securing data. GDPR now puts a duty on organisations to report specific data breaches to the ICO, and in some instances to individuals (if likely to result in a high risk to the rights of individuals). Big organisations also need to create policies/procedures for managing data breaches.

The role of Data Protection Officers (DPOS), who take responsibility for data protection compliance, will help. There are many rules in place to ensure they are not restrained by management and can act with authority. What GDPR does is force companies to adopt security practices that many good security aware companies have been practicing for some time. This law is fair. It is wise and the only ones who could really disapprove are those who seek to use personal data in nefarious ways." COMMSBUSINESS

> "Compromised IoT devices have been responsible for many large-scale botnets in recent times and this will only hinder the reputation of IoT and slow public adoption and acceptance"