Speech: Margot James speech at the IET Conference

It is a pleasure to be here to launch this important piece of work.

When you look at what makes a world leading digital economy then cyber security is a crucial component of this.

And as data driven technologies become more and more widely adopted, cyber security is an issue that should concern policymakers all across the world.

Because the consequences of a major breach could be catastrophic.

Not just to our physical infrastructure, but also to the confidence that is needed to encourage the adoption of exciting new technologies.

Simple measures can form the best protection against cyber attacks.

Which means that the solutions are in our grasp.

And that the Government can have a key role to play here too.

The Internet of Things represents a new chapter of how technology becomes more common in our homes, making people’s lives easier and more enjoyable.

Forecasts vary, but some suggest that by next year, there will be an estimated twenty billion internet connected devices worldwide.

In the UK alone, it is estimated that ownership of smart devices could rise to 15 devices per household within the next twelve months.

The cyber security of these products is now as important as the physical security of our homes. Secure by design Organisations need to be taking care of their customers.

And the most effective way to do this is to make sure the products that they produce are secure by design.

Because security should no longer be an afterthought but should be embedded within everything. Last year we published the Code of Practice for Consumer IoT Security to support all parties involved in the development, manufacturing and retail of consumer IoT products.

Companies such as HP, Centrica Hive, Panasonic and Green Energy Options have all pledged their public support for the Code and we encourage other manufacturers and retailers to follow suit.

But many of the internet-connected devices currently on the market still lack even the most basic cyber security provisions.

This is unacceptable. The Government has a duty of care to its citizens, to help make sure they can access and use the internet safely.

Whilst Government have previously encouraged industry to adopt a voluntary approach, it is now clear that decisive action is needed to ensure that strong cyber security is built into these products by design.

So today we are launching our consultation on regulatory next steps for consumer IoT, which builds on the extensive work that we have done to date with industry.

The proposals within this consultation focus on ensuring that baseline cyber security is being built into these products by design.

This is why the basis of the proposals centres around the following top three guidelines of the Code of Practice.

First forbidding the use of universal default passwords in consumer IoT products,

Second, manufacturers must ensure that there is a contact point for security researchers to report vulnerabilities

And finally, consumers must be informed of the minimum length of time for which security updates are provided for their devices.

We are advocating a staged approach to regulation which will increase the baseline level of security within products whilst also providing manufacturers with sufficient time to implement the proposals.

But mandating security requirements based on the code’s top three guidelines is just the first step in the legislative journey.

As part of our commitment to review the code every two years, we will examine whether further guidelines will need to be mandated at a later date.

We know that consumers already care a great deal about security when buying an internet connected products, but there is still much more to be done to provide consumers with easy access to important information so that they can make more informed decisions when purchasing these products.

This is why we are also consulting on a voluntary labelling scheme to help consumers do just this.

The label will highlight compliance with the above mentioned aspects of the top three guidelines of the Code of Practice and will help consumers differentiate between products that have basic security provisions and those that do not.

Ultimately, the security of the Internet of Things is a global challenge, and so requires a global effort to get it right.

Our proposals are consistent with the Code of Practice and recently published industry standards on consumer IoT security.

We are working with stakeholders in Europe and internationally to drive forward a harmonised approach to securing consumer smart devices across international supply chains.

We hope the publication of this consultation will be the start of a longer conversation about how best to approach the regulation of consumer IoT products.

We want to hear your views, along with views from those outside this room.

My officials will be holding roundtables to gather stakeholders’ views and outlined in the report are a variety of mechanisms for providing feedback.

Please take advantage of them before the 5th June deadline.

I would like to take this opportunity to thank PETRAS, NCSC, industry and the various IoT security professionals involved, including David Rogers, for supporting the Government with developing these proposals.

We look forward to continuing to work with you all to achieve this secure by design vision over the coming months

Before I go, the message I want to leave you all with is this; we don’t have to choose between innovation and security.

The two are not mutually exclusive. In fact, good security gives the stability and the certainty that businesses need to thrive.

Well thought-out and flexible regulation in this space is so critical to the health of our economic success.