Executive Summary

This report identifies the key findings which were developed during a workshop involving a number of regional micro, small and medium enterprises from a range of industrial sectors and experts in the field of cyber security and business. The purpose of this dialogue was to establish the issues that businesses classed as an SME face with respect to Cyber Security. The output from this workshop, along with this report identifies the market failures that key stakeholders, such as universities and government, need to address in order to support the industry and help to grow a secure digital economy. This workshop follows on from CSC2012 and also the report SBCSS2012 which highlighted the significant problems SMEs are facing with regard to receiving support with regard to cyber security. Security Lancaster partnered with the ICT.KTN and sought to work with a diverse group of SMEs in facilitated teams, taken through a series of guided exercises, to first and foremost identify their concerns around cyber security and subsequently capture any potential ways forward.

Key findings

In summary the following are the key findings developed from the output and discussion undertaken during the workshop:

- SMEs are in fact three different types of businesses (micro, small, medium) with different needs and cannot be treated as one sector.
- There is a need to understand that security although significant needs to be balanced against business agility and market responsiveness.
- Risk exposure and appropriate requirements are related to organisation size
- Cyber security Fear Uncertainty and Doubt is damaging giving a need for clear communication

Ultimately we propose three basic principles that should be undertaken by any organisation seeking to provide advice to businesses classified as a Small to Medium Enterprise.

1. **If you are small then Agility is more important than Security**
2. **They are not SMEs they are micro, small and medium businesses**
3. **Stop talking about cyber security start talking about digital business risk**