

Cyber scaremongering isn't working claim small businesses

May 30 2013

Stop talking about cyber security and start talking about digital business risk...that's the message coming over loud and clear from the small business industry.

A new Security Lancaster report has identified market failures that key stakeholders, such as universities and government, need to address to support the [small business](#) industry in growing a secure digital economy.

Earlier this year Security Lancaster, the EPSRC-GCHQ Academic Centre of Excellence in [Cyber Security](#) Research at Lancaster University, held a workshop involving regional micro, small and medium enterprises from a range of industrial sectors and experts in the field of cyber security and business.

The workshop, held in conjunction with London-based ICT Knowledge Transfer Network (ICT KTN), explored delegates' thoughts on business needs about cyber security and the findings from the Small Business Cyber Security Survey conducted by the two organisations.

The survey findings and workshop intelligence have just been published. It is hoped the report will help shape the debate around the support given to the largest sector in the [UK economy](#).

Key findings include:

- Cyber security fear, uncertainty and doubt are damaging and

demand a need for clear communication.

- Cyber security must be balanced against business agility and market responsiveness. When a business is small, the need for business agility is very high, to mitigate the risk of business collapse and to respond to customer needs.
- SMEs are three different types of businesses (micro, small and medium) with different needs and cannot be treated as one sector. The size of the business impacts on its nature, culture and style of operation, which is radically different between micro, small and medium enterprises.

The workshop focused on [small business owners](#)' thoughts on how organisations, such as the UK government, should support the small to medium enterprise community in defending themselves and also developing new business opportunities in the cyber security sector.

"Small to medium enterprises are key to the UK economy," says lead report author Dr Daniel Prince, Security Lancaster's Associate Director for Business Partnerships and Enterprise.

"We must support them in their defence against [digital business](#) threats, but also encourage enterprises to differentiate and diversify their products and services to provide cyber security solutions to the UK market place. Our report starts to identify how collectively we might be able to achieve this.

"The message is very much - stop talking about cyber security and start talking about digital business risk. It is clear that the language used is vital to the uptake of the advice regarding cyber security. Scaring individuals to take action is not working and is actually having a negative effect. Further, the technocratic language used to describe cyber security is counterproductive, further driving individuals away."

Tony Dyhouse, the Director of the Cyber [Security](#) initiative at ICT KTN, commented: "Over the last few years I've witnessed the rise in the amount of information regarding cyber threats being provided to UK industry from government sources. There's been plenty of best practice guidance on recommended actions issued too. Yet the number of successful compromises and financial losses being reported seemed to show that this advice was not being acted upon. This was further evidenced by our Small [Business](#) Survey in 2012. I was surprised that even cyber-savvy companies seemed not to adopt the appropriate protection being recommended. Maybe it wasn't as appropriate as we thought?"

Provided by Lancaster University

Citation: Cyber scaremongering isn't working claim small businesses (2013, May 30) retrieved 17 May 2024 from <https://phys.org/news/2013-05-cyber-scaremongering-isnt-small-businesses.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.