**NCPF IoT Special Interest Group**

# Big Data, IoT, Integration and Cyber Security

Prof Anthony Furness
Visiting Professor, Harper Adams University

Since the announcement of the special interest group for the Internet of Things (IoT) applied to Agriculture, discussions with interested parties, including industrialists, have made it clear that the interests relating to developments in big data need to be united with those concerning the development of the IoT. In many respects that was considered to be inherent within the initial proposal. However, as a consequence of those discussions the National Centre for Precision framing (NCPF), hosted through Harper Adams University, in collaboration with the new AgriEpiCentre, are now in the process of setting up an integrated interest group, currently referred to as the Digital Agri-Food Special Interest Group, focused upon driving the development of Agriculture 4.0, Big Data, Cloud-based analytics and the IoT within the UK farming sector.

In the NCPF announcement for the inaugural meeting for the group the initiative is described as "*a self-selecting group made up of GIS, Big Data and IoT companies, agronomists, farmers, agrochemical companies, machinery manufacturers, supermarkets, food processors and others interested in participating in the developing this new industry. It is anticipated that this group will create vision and cooperate in developing new ideas, joint ventures and collaborative projects with a view to creating exciting new products and spin offs. As this group will contain both farmers and agronomists, it will provide them with a voice in the development of this new industry and the chance to participate. It will also provide industry with the opportunity to educate, inform and help overcome farmer concerns over the use of farm data*".

Data, identification and the existing Internet are common to all the elements (Agriculture 4.0, Big Data, Cloud-based analytics and the IoT) identified in this integrated approach. Such integration makes sense providing that an incisive, inclusive agenda can be derived for the group that goes beyond the hype-ridden, superficial projections that have frequently accompanied these somewhat enigmatic labels. The group will have the opportunity to address the issues that will make or hinder the realisation of this Digital enterprise. It is an opportunity that requires understanding of the digital issues involved and appropriate representation to ensure the group can deal with the inherent technicalities of integration for network developments. This includes technicalities that will be largely transparent to farmers and associated food providers, but necessary to realising coherent and effective agriculturally-focused network developments that are relevant at both national and international levels. However, there are issues that cannot just be left to the infrastructure and service providers alone, including, for example, those concerning Internet vulnerability, identity, privacy, the rise in cyber-crime and the associated need to greater security.

While farmers and other practitioners in Agri-Food businesses cannot be expected to address the deeper technical issues an appropriately structured Interest Group can make a significant contribution in addressing the issues on behalf of these stakeholders and to the benefit of Internet and IoT developments in general.

The Internet was never structured for security and safety, largely reliant upon trust, the weaknesses in its structure, its development and limited governance[1] have allowed criminals to exploit the vulnerabilities and gain financially. It has been estimated that the cost to businesses of cyber-crime is some $400 billion worldwide[2] (including costs of security provision, damage repair and financial losses). A UK Cabinet Office report on cyber-crime estimated in 2011 that the cost to the UK of cyber-crime activities was in the region of £27 billion per annum[3]. This is estimated to have risen to £34 billion per annum by 2015 (£18 billion attributed to revenue losses resulting from successful attacks), with an average cost to UK companies of some £4.1 million per company[4], based upon a study of 39 benchmarked companies.

Clearly, it is not just financial fraud at work here, the rising incidents of 'malware' infection is accounting for more and more attacks on corporate assets and functionality, including data, information and intellectual property theft, and attacks upon business and production capabilities. It is not just large organisations who are targeted in attacks, according to Microsoft some 20% of attacks have small or medium sized targets[5]. While agricultural businesses do not feature largely in these estimates it would be naive to assume that the agricultural industry is immune to such attacks. Understanding the nature of these cyber-crime activities and the means to defend against them must be seen as an important consideration in the Interest Group agenda, assisting in bringing the facts to the fore and the routes to achieving more secure infrastructure and practices.

Agriculture is too important to risk any inadequate attention to the issues of cyber-security. As the IoT developments gain ground, with its inherent emphasis upon automated machine-to-machine (M2M) communications and data transfers between object-connected electronic devices, the risks associated with cyber-crime will undoubtedly increase – and evidence suggests that are increasing.

The IoT Interest Group along with or integrated with the Digital Agri-Food Interest Group have the opportunity to take a lead in putting the agricultural industry at the forefront of IoT/Big data advancements. Cyber-security is just one of the technical supporting issues that can be seen as important, along with the other, more directly commercial aspects of IoT/Big Data developments that can be exploited for business development and economic advantage.

For further information please contact: ncpf@harper-adams.ac.uk or 01952 815184.

---

[1] Furness, A (2011) International Framework for IoT Structure and Governance (CASAGRAS2 Deliverable 4.1 – A Specification of rules and procedures for governance)

[2] Lucas, e (2015) Cyberphobia – Identity, Trust, Security and The Internet, Bloomsbury
Also http://fortune.com/2015/01/23/cyber-attack-insurance-lloyds/

[3] UK Cabinet Office (2011) 'The Cost of Cybercrime', UK Cabinet Office, London, Report, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60943/the-cost-of-cyber-crime-full-report.pdf

[4] Ponemon Institute (2015) 2015 Cost of Cyber Crime Study: United Kingdom
http://cybersecuritysummit.co.uk/wp-content/uploads/2015/06/2015-UK-CCC-FINAL-3.pdf

[5]