BIZCOMMUNITY

Why agribusinesses see IoT data security as a challenge

Against the backdrop of a worldwide demand for food, a changing climate and a limited supply of water, fossil fuels and arable land, the Internet of Things (IoT) is empowering the digital transformation of the agriculture industry.

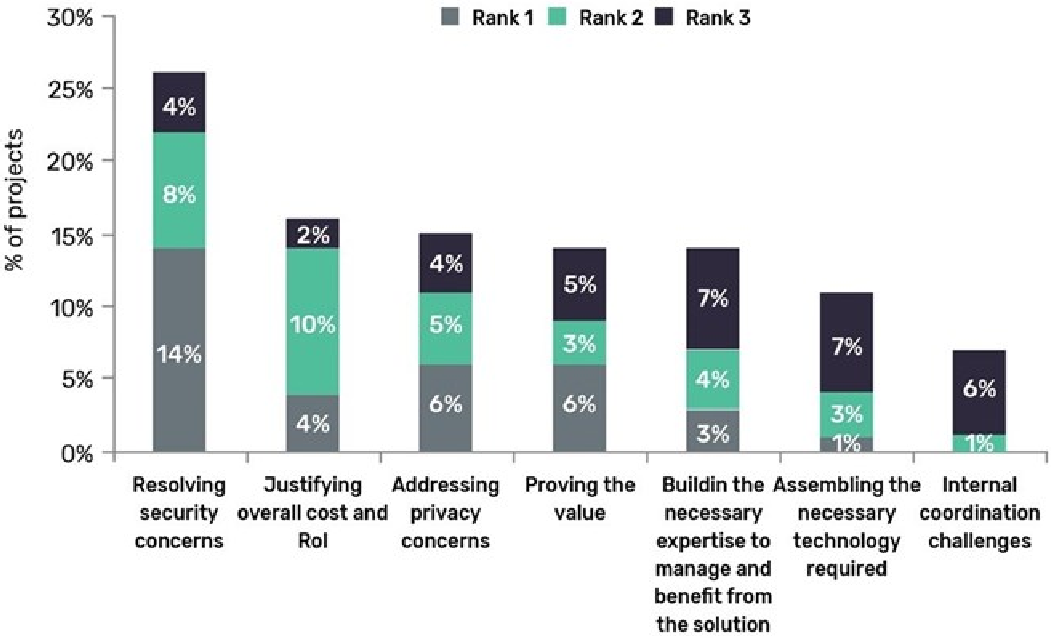
©budabar Fagan via 123RF

Data and analytics company, Global Data says that while agriculture IoT systems are growing, security issues have emerged as a major concern for agribusiness. The company's 2017 IoT project insight survey reveals that with the concept of smart farming and digitisation, IoT is gaining a significant popularity with the potential to offer high precision crop control, data collection, and automated farming techniques.

However, the farming and food chain data being generated with the implementation of IoT by farming machinery creates more entry points for hackers and leaves sensitive information vulnerable. As a consequence, many customers are now concerned about data ownership, privacy and security, which often lead to lack of confidence among customers.

This reflects in the survey findings, which show that 26% of the agribusinesses cite resolving security concerns as the most significant challenge for them.

Challenges faced by agricultural organizations in delivering IoT project



Source: GlobalData

Image via Global Data

GlobalData, senior analyst, Alok Singh comments: "IoT technology in agriculture has opened up new avenues for security incursions, with more complex and sprawling connections between components. Not entirely does each component represent an opportunity for exploitation, but, as technologies and deployments changes, they bring new threats to each component and to the overall IoT ecosystem."

The survey further highlights that justifying the overall cost and return on investment (ROI) is another vital challenge, as 16% of respondents are not clear about the costs and ROI they're going to get from IoT implementations.

Singh concludes: "While IoT systems in agriculture are growing exponentially, security issues are also surfacing at a high rate. IoT security ought to be a blend of complex security strategies and activities that must be implemented at all levels of IoT architecture. Moreover, IoT security frameworks have to be dynamic, being fit for self-learning in light of the fact that new threats to IoT appear every day."