IoT platforms increase despite security risks

A new Kaspersky report - *With superpower comes super responsibility: benefits and challenges of IoT in business* - has revealed that the use of Internet of Things (IoT) business platforms is growing year-on-year in almost all industries.
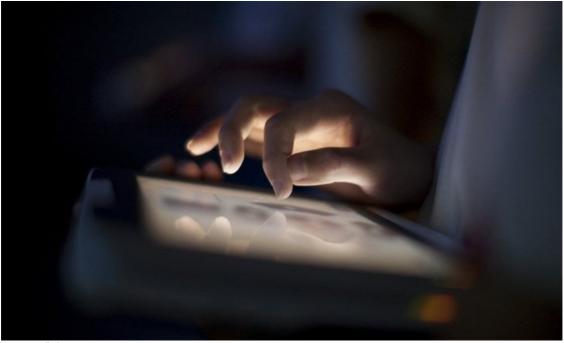

Image supplied

In 2019, 80% of companies in the META region implemented IoT applications. The technology is benefiting businesses with savings, new income streams and increased production efficiency, but the fact that 51% of META organisations experience cybersecurity incidents targeting connected devices also reveals the need to carefully protect IoT.

The internet of things is actively developing technology, with Gartner predicting there will be approximately 25 billion IoT connections by 2025. IoT increases the level of comfort we experience at home and in our cities, helps to solve resourcing issues and allows organisations to measure production performance, introduce automation and increase efficiencies.

All this makes IoT systems critical, therefore it is important to not let a failure in such systems ruin the positive impact on businesses and people.

Across all industries

Kaspersky's report shows that the use of IoT platforms has increased in almost all industries globally, with the most significant growth in hospitality (from 53% in 2018 to 63% in 2019), healthcare (from 56% to 66%), and finance (from 60% to 68%).

As of 2019, the IT and telecom (71%) and finance (68%) industries have embraced IoT more than all other verticals. IoT platforms are used in many different use cases including smart cities, grids, metering, transportation and logistics, as well as automated manufacturing and connected heating, venting and air conditioning (HVAC).

Cybersecurity concerns

The growth of IoT use has not been discouraged despite potential cybersecurity risks and incidents. As Kaspersky's survey shows, 51% of companies in the META region stated that they experienced incidents involving non-computing connected devices last year.

These incidents can be critical as sensors and smart devices collect terabytes of data, including sensitive information such as business data or customers' personal information. Also, IoT platforms can be connected with critical systems, like traffic, power or transportation processes, so it is vital to ensure their continuity and integrity.

"IIoT has clearly passed the "hype" stage – not to say there still isn't hype, but there are serious technical and business process results to apply today. The IIC has already started publishing results from our testbeds.

The biggest challenge the industry faces is resistance to change – or to be radical – more efficient change. Industrial IoT means big changes in every vertical, and they must come to terms with that," commented Dr. Richard Soley, executive director at Industrial Internet Consortium.

"IoT is a powerful business enabler but to reap its benefits organisations need to put in a considerable amount of effort. It demands dedicated business processes, as well as expertise, to ensure it is effectively implemented. As the survey shows, cybersecurity is also a question that needs resolving in the IoT space — in terms of security of equipment, technical and organisational protection measures and data privacy, as well as other factors."

"It is important to consider security at an early stage of IoT implementation and we want to help our customers address this task by developing IoT security solutions and expertise within Kaspersky," said Grigory Sizov, head of KasperskyOS Business Unit, Kaspersky.