



The Promise, Challenges and Solutions Around IoT

IT leaders share concerns and optimism for the possibilities around the internet of things.

NEARLY 80% OF ENTERPRISES

are in the early stage of their internet of things (IoT) journey, while 20% say they have reached maturity with their implementations, according to a [2020 survey from The IoT Magazine](#). This IoT journey — including challenges, opportunities, and solutions — was the topic of a recent virtual roundtable hosted by IDG and sponsored by Software AG and eBase Solutions.

During the roundtable, IT leaders from a variety of industries — including healthcare, government, public transit, financial services, law, and logistics — discussed their experiences, hopes, and challenges with IoT.

The executives said their organizations are using IoT in differing degrees. A hospital, for example, is working to determine how they can integrate the technology with legacy medical devices to better manage patient alerts without exposing security vulnerabilities in old operating systems.

A logistics company, on the other hand, has been working on a large IoT deployment for years to gain inventory and distribution data. Among the challenges it is facing is the need to overcome cultural resistance to change, which is slowing down business value realization.

The attendees shared several common concerns, including

- ▶ Security and privacy
- ▶ Integrating IoT with other business systems
- ▶ Capturing and retaining data

Security and privacy

IoT produces enormous amounts of data that must be protected. There are hundreds, and even thousands of devices in the field, and enterprises are concerned about securing all of them. One government CIO expressed concerns about data leakage, given how sophisticated actors can draw immense insights from minimal data. And for hospital systems, patient safety literally depends on the security of IoT on medical devices.



“Manufacturers could make that data available via APIs for a fee, which their customers and partner eco-system would gladly pay because of the value the data provides.”

— Dennis Passmore, partner at eBase Solutions

In addition, healthcare participants in the roundtable expressed concerns about data privacy, particularly when it comes to HIPAA, high trust, and GDPR compliance. Similarly, a financial services CIO noted that deployment of IoT has been delayed because it's unclear how the industry's large regulatory burden will affect it.

“Network segmentation is one of the keys to securing IoT data,” said Dennis Passmore, partner at eBase Solutions. By segmenting the IoT device network from the enterprise network, he added, it's easier to manage security and prevent data leakage.

Also, it's critical to identify and understand IoT device outliers, said Sean Riley, vice president of global industry solutions at Software AG. “Exact impersonation of device profiles is difficult. Duplicate devices are another set of exceptions to capture and manage. Updating firmware automatically helps put you one step ahead of those issues.”

Integrating IoT with other systems

IoT integration, especially with legacy systems, can be tricky and complex. However, it's important to get it right because poor integration can introduce security vulnerabilities. As a financial services CIO said: “We're still struggling with interoperability issues from the manufacturer because there's not a conformed standard.”

Another integration aspect: Enterprises rarely operate alone today. Instead, they interact with partners to form a value ecosystem. Within that ecosystem, all partners stand to benefit from sharing IoT data. One payments software CIO explained that his organization would like to get data from their hardware systems partners to diagnose the cause of customer problems more accurately and improve software performance and reliability.

“That's a revenue opportunity for the hardware vendor that they may not be aware of,” Passmore said. “Manufacturers could make that data available via APIs for a fee, which their customers and partner eco-system would gladly pay because of the value the data provides.”

Capturing and retaining data to produce value

IoT data is only valuable if it provides insights on which organizations can act. In some cases, that process needs to happen in real time, such as with a hospital system that must capture accurate medical alerts without them getting lost in the noise.

In other cases, the data can be analyzed later to produce insights over time. Predictive maintenance, for example, analyzes IoT data to identify patterns that indicate maintenance will soon be required. A public transit CIO expressed interest in this IoT model, saying his team could identify and address potential mechanical failures before they put a bus out of commission. Ideally, these alerts would automatically trigger both a maintenance ticket and parts orders to produce additional efficiencies.

Getting on the IoT journey

Passmore and Riley concluded the CIO roundtable with best practices for ensuring IoT success.

“Understand the desired outcome before you begin,” Riley said. “Recognize the benefits you need to deliver, and that will dictate which tools you use. Don't start with IoT and then go looking for a problem to solve.”

Whatever tools you choose, make them as useful as possible for everyone, regardless of their technological expertise. “The more self-service your platform and tools can be, the more you'll reduce issues associated with technical staffing,” Passmore added.

The promise of IoT is vast, and it serves as the foundation for many digital transformation projects. With careful preparation, a strategic approach, and a strong partner, enterprises can realize that promise to optimize and automate their operations.

[Click here to learn more.](#)