Creating the Workplace of the Future With IoT

CHALLENGE

Agencies spend billions of dollars annually to operate and maintain buildings

How and where government employees work has drastically changed over the years, thanks to smart technology and alternative arrangements such as telework. Some agencies are even investing in functional office spaces as a recruitment tool and a perk to keep current employees happy.

But creating workplaces of the future requires more than a knack for thinking of futuristic ideas to revamp office spaces. This movement requires agencies to take a hard look at data — from heating and cooling costs to occupancy rates — to think through security implications associated with sensors and connected devices and rethink how they manage brick and mortar facilities.

Consider this: The federal government spends billions of dollars annually to operate and maintain its massive portfolio of buildings. As the largest real property owner in the country, the federal government owns courthouses, offices, warehouses, schools, hospitals, laboratories and more.

The General Services Administration (GSA) acts as the government's landlord and functions much like a real estate organization. Specifically, GSA's Public Buildings Service (PBS) designs, constructs and operates a portfolio of buildings that house more than 1 million employees, said Phil Klokis, Associate Chief Information Officer for PBS.

Speaking at IBM's Think Gov 2019 conference in Washington, D.C., Klokis shared that how efficiently or inefficiently a building operates has major implications for the tenants and can greatly impact an agency's budget.

PBS manages 360 million square feet of office space, which includes 1,500 owned buildings and 8,000 active leases. Those buildings consume a massive amount of energy, including gas, electric, water and steam.

With so many variables that impact building efficiencies, agencies need a secure and reliable way to manage facilities based on sound data.

SOLUTION

IoT sensors and data help agencies track building efficiencies and create smart workplaces

GSA's quest to create workplaces of the future began with a metering system. Klokis will be the first to admit that it isn't the sexiest topic, but back in the early 2000s the ability to understand energy consumption was revolutionary for the government.

From there, the agency took a deeper dive to understand how key assets, such as the HVAC systems, within those buildings operate and whether they are doing so in the most efficient manner.

In 2012, GSA awarded IBM a contract to develop and install advanced smart building technology in 50 of the federal government's highest energy-consuming buildings. The effort has expanded since then and is part of a larger smart building strategy called GSA Link. The goal of the contact was to connect building management systems to a central cloud-based platform and improve efficiencies, which has saved GSA up to $15 million annually.

"We gave them insights into the operations of their buildings that they never had before and the ability to track a portfolio of buildings across the country," said Carolyn Marsh, Client Executive at IBM U.S. Federal.

About 85 buildings are currently in the GSA Link program, and each has 31,000 monitored components. Klokis explained that getting to this point required GSA to collect and normalize the data first.

This involved applying analytical rules around sensor data to give building operators new and deeper insights, said Marlon Attiken, Partner at U.S. Public

SOLUTION CONT.

Service, Watson IoT. GSA was able to put that data to use by running algorithms and understanding normal occurrences and an acceptable range of how those assets should operate.

According to Klokis, the agency collects 171,000 unique data points from those 31,000 assets. Those data points are tracked at different intervals throughout the day, so GSA collects about 35 million data points a day, he said. When agencies better understand how buildings operate, they can make data-driven decisions to improve efficiencies.

"They have now streamlined how building operators can detect abnormalities in buildings and have incorporated that change into their workflows," Attiken said. "They don't have to rely on intuition or gut reaction."

At GSA's 1800 F location in Washington, D.C., the agency literally knocked down walls and created open, smart office spaces. There's a smart lighting system, a system to reserve desk space and sensors in the windows and blinds to take advantage of natural lighting.

But workplaces of the future are about more than installing smart technologies. Determining how best to secure the IoT sensors that make facilities smart must be a top consideration. That's why the National Institute for Standards and Technology (NIST) released a draft discussion paper "to help identify core IoT cybersecurity capabilities that are most vital for Internet of Things (IoT) devices," according to the document.

"A big part of the challenge of using IoT is using it securely," said James St. Pierre, Deputy Director, Information Technology Laboratory at NIST. "This document is a conversation starter on how do we move toward a baseline" for securing IoT devices." The expectation is that this baseline could serve as a foundation for securing IoT across varying sectors and device categories.

Among the minimum IoT capabilities, NIST proposes is the ability for IoT devices to log pertinent details of its cybersecurity events and make them accessible to authorized systems and users, as well as the ability to use cryptography to secure its stored and transmitted data.

To advance the development of secure, modern workplaces, agencies must strike the right balance between embracing IoT innovations and aligning them with federal security standards.

TIPS FOR SUCCESS

1. **Creating workplaces of the future is a journey.** It begins by understanding how much energy your facilities consume. Technologies such as smart metering can help.

2. **Once your system is in place, you can begin collecting and normalizing data about your facilities.** This allows you to understand normal occurrences and an acceptable range of how key assets, such as the HVAC, should operate.

3. **Security must be at the forefront.** Treat IoT sensors with the same attention to security as any other device. For example, can IoT data be encrypted?

PROJECT OUTCOMES

85 buildings
are currently outfitted with sensor technology to monitor key assets within those facilities

31,000 assets
such as HVAC and other components, are being monitored within those 85 buildings

35 million
is the number of data points GSA receives daily about how key assets within the buildings are performing

ABOUT IBM

At IBM We confront the world's most challenging cybersecurity problems and passionately protect the faces behind the data – your citizens. Through the intersection of AI, intelligent orchestration, the agility of the cloud, and collaboration with each other, we can tackle the cybersecurity challenges ahead of us.

For more on cyber, visit us at www.ibm.com/federal/cybersecurity. Or for more about AI, IoT, cloud and government, head here https://www.ibm.com/cloud/government.