www.pipelinepub.com
Volume 21, Issue 9

Why DIY IoT Could Derail Your Digital Strategy

By: Jeff Noska

Amidst the boom in technological innovation, including artificial intelligence (AI), automation, and the Internet of Things (IoT), more organizations are embracing digital transformation than ever before. Research shows that 61% of business executives recognize digital transformation as a top priority for their organizations. This motivation to prioritize digital transformation stems from its incredible benefits, such as cost reduction, better operational efficiency, longer-lasting assets, expedient and accurate data analysis, greater customer satisfaction, etc.

In industrial settings, for example, IoT, AI, machine learning, computer vision, etc., help boost performance drastically inside facilities. Applications like predictive maintenance for essential equipment allow operators to catch problems with machinery before they break down and wreak havoc on operations. By intervening and making repairs, factories can ensure uptime and minimize downtime. Moreover, advanced data analytics shed light on unknown deficiencies, streamlining necessary corrections that optimize productivity and eliminate errors. These use cases also reduce the need for manual, human input, permitting critical personnel to focus more time and energy on value-generating projects. Of course, digital transformation goes beyond factories. It touches many other industries, like financial services, healthcare and retail—in fact, there are more than 18 billion connected IoT devices in operation around the world today.

The widespread adoption of advanced technologies like IoT means one thing: digital transformation is no longer a minor adjustment meant to gain a slight competitive edge but a strategic imperative in the modern age. While it is paramount that companies pursue digital transformation (if they haven't begun already), it is important to caution about a growing trend with IoT implementations that can derail larger digital strategies. For the sake of simplicity, this article will refer to this concerning phenomenon as "do it yourself" IoT or DIY IoT.

What is a DIY IoT Project

The origin of the phrase "DIY" goes back to the 1950s to describe home renovation projects undertaken by nonprofessionals, but has since grown to include music, arts, crafts and publishing. In the world of IoT, a DIY IoT deployment is one in which a business plans, builds and implements a project in-house, often without involving specialized vendors or external experts. The company assumes the responsibility for every project element, including selecting the hardware (sensors,

actuators, microcontrollers, etc.), developing the software, setting up the connectivity, managing data storage and processing and upholding system security.

The appeal of a DIY home project and a DIY IoT project are quite similar for homeowners and businesses, from greater control and freedom to affordability and customization. While the appeal of having greater self-sufficiency over an IoT deployment may sound tempting, the truth is that implementing and maintaining IoT solutions can be tricky. A successful DIY IoT project will require significant technical knowledge and resources. Many organizations, seeing the opportunity to save money, opt for self-managed methods despite their IT teams not possessing all the requisite skills or resources for the project.

The Challenges and Risks of DIY IoT Projects

Some challenges that companies undertaking DIY IoT projects face include inconsistent connectivity, which means unreliable performance. Specialized technical expertise is necessary to ensure IoT devices and their networks run smoothly and effectively. Organizations will also find that scaling a DIY IoT project from proof-of-concept to a fully operational system can be difficult, especially as the number of devices and data points grows. Interoperability is another common hurdle for DIY projects; specifically, integrating devices from different manufacturers and platforms can be challenging due to varying protocols and standards. Device lifecycle management (e.g., provisioning, ongoing maintenance, upgrades, etc.) is challenging without an IoT device management platform.

Another notable risk of a DIY IoT project is that costs can spiral out of control without clear benefits. Recall that affordability is one of the perceived benefits of such an undertaking because the investment in a third-party vendor's platform or solution may seem higher in comparison. However, this notion couldn't be further from the truth. The total cost of ownership for a DIY IoT project in a factory setting can be almost four times higher than adopting a third-party industrial IoT platform. Additionally, many organizations that go down the DIY route don't anticipate the ongoing costs of developing, testing and maintenance, not to mention the continuous investments in an IoT system's security and new features. Should a business not plan accordingly, these expenditures can easily balloon, negatively affecting any positive monetary outcomes the IoT deployment would have had. Depending on the complexity and scope

of an IoT application, development and deployment could take several months to a year or longer. This same time frame may not be the case for a DIY IoT project, especially for unprepared or non-digitally native companies that lack key skills. Ultimately, as a DIY IoT project drags on with no return on investment (ROI), organizations risk compromising their overall digital transformation strategy.

Risks Continued: Security

Security is perhaps the most serious risk of any DIY IoT project. When an unprepared company without in-house technical expertise embarks on such an endeavor, it exposes itself to significant security risks. Consider that 82% of IoT devices get targeted within five minutes of being connected to the internet, and 60% of IoT breaches happen because of outdated firmware. Some common mistakes a company that lacks the proper knowledge and experience to design, configure and maintain secure IoT systems make include default and non-unique passwords, unencrypted data transmissions, or insecure communication protocols. These critical vulnerabilities, inherent in many IoT devices, create easy entry points for cybercriminals to infiltrate networks, steal sensitive data, or manipulate devices.

The consequences of breaches vary from financial loss to reputational damage. Another consequence of having unsecured IoT devices is regulatory penalties. In industries like healthcare, IoT projects must comply with various data privacy, security and device standards regulations. A compromised IoT

device in a hospital setting could threaten patient safety by disrupting life-support systems or exposing confidential medical records. Likewise, in industrial environments, attackers could exploit unsecured sensors or controllers and wreak havoc across factories, potentially causing bodily harm to workers. Failure to meet regulatory standards is not only costly but possibly dangerous. Moreover, as with the previous challenges, cybersecurity disruptions will slow or outright prevent digital transformation.

Why Work with an IoT Vendor?

To truly realize the benefits of digital transformation, organizations should seek out IoT vendors that can provide holistic services beyond the device itself. An IoT deployment consists of multiple elements, including (but not limited to) connectivity infrastructure (such as cellular, Wi-Fi, or LPWAN networks), cloud or edge computing platforms for data processing and storage, middleware for device integration, analytics engines to derive insights from data and security solutions (both physical and digital) to protect against unauthorized access and data breaches. Ideally, a qualified IoT vendor will have expertise in all these disciplines to facilitate a successful and long-lasting deployment.

Working with an IoT vendor minimizes the unexpected, meaning variables like cost and timelines are much more predictable. An experienced IoT vendor can anticipate challenges and deployment risks and make efforts to avoid these potholes. For example, a seasoned vendor will proactively address interoperability challenges so data flows efficiently from device to cloud. Most vendors provide long-term support, ongoing maintenance services and scalability planning. Best-in-class vendors will likewise offer robust security solutions, including built-in device security and automated security monitoring and remediation via an IoT device management platform so that only authorized devices and users can access the network. An IoT vendor's combination of IT, engineering and security expertise will not only accelerate time to value but ensure the project meaningfully contributes to the larger digital transformation efforts.

It is also worth pointing out the value of working with an IoT vendor that provides an IoT device management platform because of it can remotely access, diagnose, monitor and manage the functionality and status of deployed IoT devices. Such a platform is especially important for IoT deployments with devices in hard-to-reach locations, such as wells, mines, or street lights. Without an IoT device management platform, technicians must manually and periodically check on those devices to update their capabilities and intelligence with firmware updates or download security patches.

Ensuring Digital Transformation

Though attempting a DIY IoT project is tempting (and maybe exciting), the consequences are too serious to risk without having all the necessary resources, expertise and personnel. Even if a business feels that it possesses these requirements in-house, it is wise to conduct an internal evaluation to see if and where deficiencies exist. Ultimately, allowing a trusted partner to assist with an IoT deployment will result in measurable ROI and scalable use cases that bolster digital transformation initiatives.