Interview

DAN LEVINE | CEO, CytexOne

IIoT Challenges and Promises

To get an idea of the challenges facing the Internet of Things, we talked with Dan Levine, CEO of CytexOne, New York City. Levine's firm creates automated Internet of Things (IoT) environments for commercial, industrial, and residential spaces, including insurers, restaurants, hotels, and apartments.

Security is a major concern with the IoT. Any idea how companies will be able to provide it?

IoT security involves protecting access to the equipment, such as an internet-connected car or house, as well as protecting customer and company data. It is, in my opinion, a failure where there is a measurable chance that equipment and data could be susceptible to hackers. Not only can equipment be damaged, infiltration can create a dangerous hazard and interfere with or downright cripple production and business process. A strong system and network designer are critical, as are robust design and ongoing monitoring.

With customer and company data stored in the cloud, a totally different type of security is needed. That security must be provided by the IT team storing the data, and to do a good job, the IT team must include a solid team of security experts who stay on the cutting edge and ahead of common technology.

It's said that locks and security are really not meant to stop anyone from breaking in, just to slow them down. And most people do not try to break into something that's locked. But if they really want to—and have the time, money, and motivation—they can. Not many hackers will break into a single piece of equipment or device unless it is sold in high volumes to consumers or industry, and not unless their action will cause meaningful disruption. That's why consistent, reliable monitoring is critical not just for systems, but for systems of systems as well as individual devices.

How will companies solve these security issues?

Some companies will be better at it than others. IoT is dynamic. There will necessarily be many different security products and vendors. End users and interim management companies—and even IoT service providers and designers and companies—need firms like CytexOne because they offer services to guide; insulate; protect and proactively monitor; and repair systems and potential pitfalls of what can otherwise be a security minefield. Successful companies will include real-time monitoring of the security and vulnerability of their networks; constantly scan and analyze security and performance; and—most importantly, repair—all in real time.

Does the IoT need unifying standards for issues such as security, interoperability, and performance?

Unifying standards would be helpful in that they would increase adoption levels and remove the temptation or perceived necessity of reinventing the wheel, and avoid wasting time rediscovering the failures others have already experienced. On the other hand, a tight unifying standard may limit innovation. We are in an era of endless innovation with technology, much like the machine age of the 19th Century. It's just imperceptible to many people. To establish market share, a great product and service are necessary, and those come only from innovation and devotion to the cause.

That is not to say that unifying standards won't make it easier to find, track, and avoid security vulnerabilities. And once a vulnerability is found in hardware or software, unauthorized access to many sites is possible. For example, a bug that came out in Android could be widely exploited by hackers. If they could get a text message with certain characters in it to the phone, it would give them full access to the phone. To complicate the problem, the open-source nature of Android and the fact that the phones don't all centrally update makes it difficult to patch the bug. There are many phones still totally vulnerable.

There are certainly some standards in IoT, such as the wireless frequencies used (ZigBee, Bluetooth, Z-Wave). But in the software-stack arena, it has been like the Wild West. There are so many different platforms, and many do not last a long time. A company can invest and deploy a platform that seems great and works well, but then if the company that developed and supports the platform goes out of business, that platform is effectively dead.

For instance, a company called Quirky developed an IoT platform called Wink that was accessible to everyone, with devices available in Home Depot, Staples, and other places. There was all sorts of money invested in the company, and then

it went out of business. All of the companies that had been using it ended up with hubs that were useless. NASA also bought a hub, Revolve, but then shut it down. Even Staples had a hub that got shut down. In the industrial sector, it is expensive, if not impossible, to retrofit one device to work with a new hub. More focused platforms, more focused communication, and more streamlined and approachable hubs and platforms are available, and companies like mine design systems and systems of systems that are secure and take advantage of available hardware.

So should there be a greater need for standards covering hubs and other critical infrastructure?

It is ideal to have certain standards. But right now, companies want to own their own platform and software. Without standards, no one really owns either. So although having IoT standards would be phenomenal, it's a difficult task. Eventually, the companies that survive will adopt a standard in the years to come, and they will be set on adoption rather than some entity mandating it. It will depend more on who buys what and what gets used more.

Who or what should establish IoT standards?

Well, we've seen that governments managing standards can be tricky. And which government would it be? The U.S.? The U.K.? And how would that government interact with other governments around the globe, especially those that might not have any buy-in behind the standard? Would it be private companies? Private equity managers who fund companies? Can it become as ubiquitous as the internet? Perhaps. I think it needs standardization like electricity. After all, the IoT is a commodity and a necessity, like electricity.

Should some non-profit organization set them?

That would also be problematic. As more people and companies join those organizations, the harder it is for the group to incorporate innovation into the standard, and the less evolutionary and open to change they become. Everyone has an opinion and agenda. And some companies have been known to use standards as competitive advantages and as a weapon in the marketplace.

So when it comes to the IoT, it will likely come down to the participants in the marketplace setting the standards.

Are there any challenges specific to the Industrial Internet of Things, the IIoT?

Many people in the industrial sector have spent a long time in their industry, and most people believe they do things better than anyone else. This sometimes leads to companies deciding to reinvent the wheel internally rather than looking externally for solutions that are already built and proven. Outside solutions do not provide the same level of job security for teams that have been working on problems for a long time. So perhaps the big-

gest hurdle will be overcoming resistance from the managers and employees themselves.

On the other hand, the IIoT is a much easier sell than the consumer side of the IoT. For a business, there's a value proposition and you can show an ROI. It's not a convenience or luxury item; it's a true ROI and competitive advantage. The IIoT should lead to reduced cost structures, increased operational efficiencies and manufacturing yields, higher quality of products (fewer defects), more efficient sourcing of materials, and lower expenses due to smaller staffs but higher output. For consumers, this means lower costs and better products.

Will all manufacturing companies go to the IIoT?

The short answer: yes. One day, everything will be connected to the internet. Everything. Even the pavement on your driveway and walls in your house will be connected to the internet in some way. It's just a matter of time. I would say it will reach nearly 100% in 100 years, and reach over 50% of things within 15 to 30 years. It's possible to do it now, but people don't realize the benefit, or the inexpensive investment for total access and environmental management, avoiding repairs, and managing energy consumption, as well as people and processes.

Will well-off, established industries be better positioned to implement IoT than startups and smaller companies and industries?

No. Just the opposite. Startups and smaller firms are more limber and robust than large companies. Some companies, like IBM and GM, are so large, with so many departments and government-like bureaucracies, that it seems that most can't be as nimble as change and innovation require.

For example, when Microsoft launched Office 365, it was reported that there was infighting and resistance inside the company from groups that had been selling Office on the desktop as a perpetual license rather than subscription license. It's remarkable that in an innovation-dependent industry, large companies that brought technology to the masses, such as Microsoft and IBM, are almost behind the curve. So it will depend on the individual company's structure and culture as to whether the institution and individual employees are willing to change.

Another related problem is that some established companies have large teams filled with groups of geniuses working on IoT technology. Sometimes they solve the problem, but often they just get bogged down. They want to build the solution themselves, internally. They feel they can do it better. But they lack the IoT experience and up-to-date technology knowledge and know only their own industry and what worked in the past. Startups and smaller companies don't have any legacy people, processes, or products. md