
CIO ROUNDTABLE:

The Internet of Things: Moving from Vision to Execution

Enterprisers Virtual Roundtable | Fall 2015

Technically, the Internet of Things (IoT) era began in the early 1980s when programmers at Carnegie Mellon connected a Coke machine to the Internet, but in the last few years the space has exploded. In June, IDC predicted that the global IoT market would grow to \$1.7 trillion in 2020. Meanwhile, Intel predicted an \$11.1 trillion market by 2025, up from \$655.8 billion in 2014.

The Internet of Things seems to represent both a bonanza of predictive insights but also – as a mesh network rather than a traditional point-to-point network – a terrifying new breed of threats to security and privacy. So how do leading IT organizations move from vision to execution while minimizing risk?

To find out, The Enterprisers Project gathered four IT executives to separate a few IoT appearances from realities.

Panelist Profiles



SVEN GERJETS

Chief Information Officer
Time Warner Cable



EAMON O'KELLY

Vice President and
Industrial Solutions Chief
Information Officer
TE Connectivity



TOM SODERSTROM

Chief Technology and
Innovation Officer,
Office of the CIO
Jet Propulsion Laboratory



CLIFF TAMPLIN

Consultant and former VP
of Technology Support and
Risk Management
Hyatt Hotels Corporation

ROUNDTABLE: The Internet of Things

IoT: Which Game Are We Playing?

THE ENTERPRISERS PROJECT (TEP):

On one hand, it feels like IoT has been around for years. On the other hand, when an IT executive was recently asked which IoT inning we were in, he said we haven't even built the stadiums yet. What are your thoughts?

CLIFF TAMPLIN: I find I'm not even sure which game we're playing. For me the question is, what is the business result we're trying to achieve? I recently was counting, and I've got 60 IP or network-addressable devices in my house: my thermostat, the cameras, the door locks, the television, pretty much everything you look at. But every device is being driven by a different business initiative. So how do we make money out of this?



Cliff Tamplin

TOM SODERSTROM: I think it's not what inning we're in or what game we're playing. I think there are a whole bunch of kids playing in the park, and we're trying to figure out what the game will become. Maybe IoT is about automation, which you can see across the home and in conference rooms and in clean rooms. Maybe it's about saving energy, or about better

situation awareness. I actually think the hype is excellent, because it drives a lot of innovation.

The good news is, it's inexpensive to prototype and surface the key benefits. In fact the cost to play the game is miniscule. It's very easy to customize the environment, and I think that's the key to this. In the end, I think it'll be the ability of end users to customize their own environments with very inexpensive hardware; that'll probably be the biggest benefit. But how do we do that securely? The cost of a security breach could be major.



Tom Soderstrom

SVEN GERJETS: For me, IoT is a little bit of an intellectual thing, because at my current role* at least, we're not really focused on devices and consumers. But I am a user of some of these products, and it's interesting where it will go. I think it's an astute point to say it's a little bit scary how easy it is to expose yourself to a whole bunch of security issues. And unfortunately, these devices make it easier to do every day.

EAMON O'KELLY: In terms of having 60 connected devices today, we'll probably be adding a zero onto that in another five years. From a business perspective it's going to be a booming area as well. We're well positioned because we're the T in IoT and enabling the connectivity.

The Internet of Hacked Things?

TEP: Clearly there are a lot of privacy and security red flags going up around IoT. One security expert recently said we're making "really horrible, horrible choices" in this regard. Is IoT a security train wreck waiting to happen, or has that train left the station and we've just got to do what we can to cover off on these issues?

CLIFF TAMPLIN: I would say there are three almost parallel threads going here. First, we have a whole bunch of application and business developers throwing technology out there, and they are solely focused on their particular piece of the cake: How do I get stuff out there? How do I get ahead of the game? How do I get consumer buy-in to what it is I'm doing?

“We're well positioned because we're the T in Internet of Things.”

In parallel, there's the old IT operations that, as always, is playing catch-up with the developers, figuring out how to make this stable, how to make it secure?

And then finally, following along behind that, we have the lawyers. Given everything that we're doing in this particular case, because it's touching the consumer in so many different ways, I think it will be 10 years before they catch up to the implications of what's going on. Imagine someone uses my smart fridge as a gateway to hack my electronic safe, and opens that and steals all my stuff. Who do I sue? All this is touching people who don't understand the implications, don't understand

ROUNDTABLE: The Internet of Things

what's going on, and frankly don't have a cat in hell's chance of protecting themselves against this.

TEP: Cliff, are you being called on to help your clients define Internet of Things as a strategy or is it much more kind of tactical and product-to-product driven than that?

“

I think a complete shift in the way revenue is going to be created is the upside of all of this.

”

CLIFF TAMPLIN: Generally, I don't hear people talking about Internet of Things other than the marketing people. Where I get involved in things is how do we productionize this great idea we've got. And they tend to be very siloed. I've been working with somebody on point of sale and how we're linking point of sale out to monetize what is going on in a hotel room, what's going on in a bar, etc. - linking all of those things together so that we can beacon people and track people and we can identify them as they're going through physical locations. That tends to be very much focused on the particular industry and a particular client. I don't think anybody I'm working with is taking in the big picture.

TEP: So at this point it's more about connectivity?

CLIFF TAMPLIN: Yes. The business people want ubiquitous connectivity, and the IT people are saying, "How do I maintain connectivity when somebody goes into a subway?" but also, "How do I maintain connectivity when I don't have the source code for these sensors that we're putting

out there?" So again, I do a lot of work with lawyers. And they want to know, "How do we protect ourselves against IP infringements where we're dealing with somebody but nobody knows where the code came from?"

IoT Meets IT

TEP: Given what we're hearing about network and storage demands from IoT, what kinds of forces are you feeling in your IT departments because of this new wave of devices?

EAMON O'KELLY: One area we're looking at is analytics platforms. We're obviously moving away from the traditional database world to Hadoop to allow us to have scalability because we expect to have 10 or 100 times more data in our data lake. That's probably the same parallel with IoT. If you have 60 devices in the home with reference points all pushing out digital exhaust, it's got to go somewhere, right? So our move is to try to leverage more of the open source scalable solutions, rather than the traditional stuff.



Eamon O'Kelly

TEP: Tom, how have you seen demand for different capabilities change as the nature of these devices evolves?

TOM SODERSTROM: Well, IT can never change faster than human behavior lets it change. And those human expectations of IT are being driven by the IT consumers have and can play with at home. So how do you take that into the enterprise? When we looked at that, we saw that the real trend here is the disruption of the enterprise, where all of these consumer things are being expected in the enterprise. IoT is driving that in a big, big way, from all the Apple watches to these new devices that the people have at home.

“

Everything talks to everything else. And when that happens, our perimeters and the things that we always thought of being able to control we can't control anymore.

”

To respond, we came up with something we called E4, which stands for Engage and Enable Everyone and Everything. And the Internet of Things is at least a quarter of that. So we're using prototypes to look at the use cases. For example, we stood up the new lab that we called the Innovation Experience Center, and the idea is you come in here to experience the future, part of which is IoT things like lights, motion sensors, and holograph in a fairly small startup environment.

To do all that safely, we have to start with security. And we created a new device network that all these devices live on, so they're not connected to the JPL network. That created a lot of excitement and is helping drive collaboration with the end users. The overall benefit is people can customize their own environment easily

ROUNDTABLE: The Internet of Things

and quickly, for situational awareness.

The net is, IoT is going to drive things like software-defined networking. How do you set up a network across JPL to all these devices and to the cloud? Chaotic architecture, because enterprise architecture just doesn't work anymore. How do you adjust to it? Big data analytics. IPv6 is all of a sudden becoming much more important. Cybersecurity is, of course, paramount. I think it's just for us to figure out how does it benefit us. And it'll probably come in different varieties. But even within a week of playing with it, we found all kinds of use cases where people can see it. So long answer, but have to let people play with these things. Just be overcautious on security.



Sven Gerjets

SVEN GERJETS: A question to the group on the security front. In all likelihood, one of the big companies is going to get hacked. Say Nest gets hacked, and all of your video footage gets taken. Do you think it's going to change the disclosure laws there? A related question is that since most of the consumer devices are kind of spun up by different companies, how do you tackle security when you've got 100 different credit cards all managed by different banks and you just have to rely on them to be secure at some level, right? Is there something coming where there's going to be almost some middle security layer between the

providers and the home? An encryption layer, a key repository layer or something?

TEP: A security middleware?

SVEN GERJETS: Yeah, exactly.

SODERSTROM: I can talk about how we do it in the enterprise. We talked about it for four years, but it finally made us create the device network and an incubation network, so we could put all of these new devices on the incubation network. They're not supposed to talk home or leak. And now we can measure it because it's off the normal network. If we leave them there for a month or so, we feel at least we have characterized them. So that's inside the enterprise, where cybersecurity is part of it. Outside, I don't know. It's a really good question.

“

Imagine someone uses my smart fridge as a gateway to hack my electronic safe, and opens that and steals all my stuff. Who do I sue? All this is touching people who don't understand the implications.

”

Where Can IT Lead in IoT?

CLIFF TAMPLIN: The question I would ask you on that is, how do you know that you've got everything contained? To me this stuff is almost like a Star Trek-type virus, not in the technical way that we think of computer viruses spreading but in the way that people, without understanding what's going on, bring in devices

that they may not even know are capable of connecting. Then those things pollute and corrupt our networks, and circumvent the technology that we're trying to put in place.

I recently bought a smart television. The first thing you find when you get this thing is that there's about 20 pages of legal disclosure before you can actually use the television, which basically says that the manufacturer isn't responsible for anything, and it's all my fault. The next thing I discovered is that this TV is pulling and hooking onto anything and everything that it can find. I'm still trying to understand all of what it's doing. It's in my home, and it's taken the place over. What happens when somebody who isn't technologically sensitive gets something like that? They click "agree" without reading the terms and conditions. They don't know how to set the parameters on it. All of a sudden, their house is gone. That's the big concern I see of what's going on.

TOM SODERSTROM: I think the opportunity here is for IT to lead. So instead of disruption, if you see it coming and you are proactive, then it's a benefit. It's going to disrupt you regardless, and I think that's what IoT is.

CLIFF TAMPLIN: So may I play devil's advocate? You have authorized devices that are on your JPL network. I suspect that the authorized devices are also capable of talking to non-authorized devices. So that, I would suspect, is the way that stuff that shouldn't be on your network will get into your network. And I mean this about networks in general. By definition, the Internet of Things is a mesh network. It's not a point-to-point network like we're used to in the past, where there's a point of control. Everything talks to everything else. And when that happens, our perimeters and the things that we always thought of

ROUNDTABLE: The Internet of Things

being able to control we can't control any more, and that's a strength but it's also the weakness.

TOM SODERSTROM: Even as I say I think we'll be able to control it, I know it's big, wishful thinking, and I'll probably fall flat. I think we'll be able to control it on the IP side. We can measure it. We can look at it. But I think you're right about the danger of the Bluetooth side. You have all these devices connecting to your smartphone. The smartphone is authorized. But it could easily leak that way. Perhaps your smart glasses are sending information to your cellphone, and the cellphone is connected to the network.

“ *I think a complete shift in the way revenue is going to be created is the upside of all of this.* ”

CLIFF TAMPLIN: I hope I'm wrong, but it scares the bejesus out of me.

TEP: You make an important point, Cliff. Originally, the Internet was about connecting people who already trusted one another. Then it goes to three billion users and it sometimes seems that all we have are stopgap measures since trust can no longer be assumed.

IoT: Where's the Upside?

TEP: I thought it was interesting that among people who were surveyed and owned smart devices for their home, 9 out of 10, despite all the risks and despite potentially giving up a lot of privacy,

would recommend any of the home devices they have to other people. And for instance over at Monsanto, where the CIO is an Enterpriser, they're using a new application they call FieldDrive, which lets them dynamically pull yield data and positioning data off of combines and tractors. They combine that data in the cloud with weather forecasts and other kinds of information, and they get very reliable reads about the quality of the seeds they're growing and where they are at the time of harvest and so on. So there's certainly a lot of potential optimism about this. What gives all of you cause for hope that we're entering a world where computers are going to kind of act on our behalf for good rather than evil?

EAMON O'KELLY: In the last half of the example you gave, they're seeing much higher utilization of their capital investment, right? I think they can also predict when a machine goes down, and if a machine goes down, it costs them tens of thousands of dollars a week. So they can proactively fix them. I know at my last company we saw a massive adjacency where we moved from a discrete product sale into a continuous service sale because of IoT. I think a complete shift in the way revenue is going to be created is the upside of all of this.

“ *I actually think the hype is excellent, because it drives a lot of innovation.* ”

CLIFF TAMPLIN: Absolutely. Just look at an early-ish implementation of the Internet of Things in the hotels market where the thermostats in the room blocks and the power controls in the rooms all talk

to each other. When you go out of your room, it powers the room down. The savings across 100,000 hotel rooms of doing that is immense. A relatively recent step is to take that isolated room and link it to the property management system so that we actually know when there's a guest checked into the room. But there is also bad news for the housekeepers: they go into the room and it doesn't turn the air conditioning on. They get to work in the heat.

“ *IT can never change faster than human behavior lets it change. And those human expectations of IT are being driven by what the IT consumers have and can play with at home.* ”

TEP: So there are ethical elements to consider in Internet of Things as well.

EAMON O'KELLY: If you take your example up a step, Cliff, and start to aggregate all of those little tiny data sets, whether it's in a home or at sports events, you can start to consider smart metering and smart utilities, where we can now push more of the power utility load to the renewable side and thin down the carbon side. That, of course, has a massive impact from a greenhouse standpoint and everything else. Not only do you have better visibility into what you need (from a capital investment perspective) but you can actually start driving behavior at the consumer level that massively benefits society at the end of the day.

ROUNDTABLE: The Internet of Things

CLIFF TAMPLIN: Indeed so. As I said, I've got my house pretty much wired, and so I've replicated what we do with the hotel room with my house. When we go out, the house powers down. When we come back in, it powers up. I'm keen on the electricity bill savings. Those are the sorts of things, when you can make that easy for people, this will have benefit to the individual. But to your point, if you then take that data and feed that back via a smart meter, that gives the local electricity utility a chance to learn about my profile and to adjust the load for the community, which, again, has potentially far bigger benefits.

“

It's a little bit scary how easy it is to expose yourself to a whole bunch of security issues. And unfortunately, these devices make it easier to do every day.”

TOM SODERSTROM: That's a great example, because you did this for your home. But if we can take all the expertise inside of the enterprise and apply it, you don't have to pay for it. It's already there. And then you get this invisible army of people who are able to customize our work environments, so we save energy, we save water, and so on. And people are really intensely interested in it because it affects them personally. We can then apply that in the enterprise, and we can do it quickly. And then once you do that, there's no problem in getting budget to do it on a bigger scale.

TEP: So even though the potential downside is still a little bit unforeseen, given that all this data hasn't come together quite as seamlessly as people thought, and there's a lot of stuff even today in the press about that, maybe we have to look at it a little bit like credit card fraud. Given the rules of chance, it may just happen at some point. It would be impossible to have 100 percent security in anything anymore.

CLIFF TAMPLIN: The point I would make there, though, is that the banks are on the hook if your credit card is misused. In the case of all this technology we're putting out for people, there's no protection. If I screw up and my house gets hacked, it's totally down to me. There's nobody else. But I just think what happens if it's my mother or a couple of my neighbors, who are technically challenged, and we could see a lot of people getting really hurt. If that happens, I think that will give us a bigger problem in terms of the credibility of the technology.

TEP: Yes. And to your point another writer I was looking into said about IoT, "How about not doing a thing just because we can?" But as we've been discussing, the train has left the station and the only real substantive response to that would be just going off the grid entirely, which is not a tenable solution. As you said, Eamon, we just have to play to this whole trend as fast as we possibly can.

* Sven Gerjets was CTO at Person when he participated in this roundtable. He recently accepted a new role as CIO of Time Warner Cable.

MAKE IT HAPPEN
COMPETITIVE EDGE
RELIABILITY
INTEGRATION
EVERYTHING
RELATIONSHIP
EFFICIENCY
CHANGE AGENT
FLEXIBILITY

CHIEF **ADAPTABILITY** OFFICER

COLLABORATION
STRATEGIC
INNOVATION
SCALABILITY
DELIVERY
INSPIRATION
EVERYWHERE
COMMUNITY

THE **ENTERPRISERS** PROJECT

Today business demands more from the CIO than just "Information." Join The Enterprisers Project, sponsored by Red Hat, a community-powered conversation that's exploring the evolving role of CIOs as they drive business strategy and inspire enterprise-wide innovation.

Articles, videos and insights at **EnterprisersProject.com**

THE
ENTERPRISE
PROJECT