What Public Sector CIOs Must Consider in Preparing for Trusted IoT Deployment

By Kathy Stershic, Principal Consultant, Dialog Research & Communications

Public Sector CIOs are facing unprecedented opportunity with the emerging Internet of Things (IoT) paradigm. How can and should they prepare to take advantage of IoT, while creating a secure, trusted foundation for the long term?

Gartner defines IoT as "the network of objects that contain embedded technology to communicate and sense or interact with their internal states or external environment." At present, that generally means a machine-to-machine connection, although an expanded 'Internet of Everything' may well evolve to include people-to-machine and process-to-machine connections in an ever-growing ecosystem.

While select commercial applications are beginning to appear, at this very early stage IoT is one area in which Public Sector IT has a unique opportunity to lead—creating large scale deployments driven by constituent demand, growing security threats, and the economic imperative to "do new with less." For example, smart street lighting solutions can reduce crime while saving money; combined water management, smart grid and waste management can yield greater ROI on energy investment; connected warfighters can bring dominance to the battlefield, faster.

While the opportunities are many, so are the risks. IoT presents exponentially increased threats in a dynamic landscape. There *is* no more network perimeter. Embedded, non-standardized sensor hardware creates an increased number of connected threat points, many of which will result from the 'smartification' of traditionally dumb devices never intended for software or IP and built by manufacturers not accustomed to thinking about digital security.

There is a pending vast amount of data to be generated by new sources—how must it be secured as it moves and permutates? The public internet is highly vulnerable, but even isolated networks are not impermeable— think back just a short time to Stuxnet.

Human error is a leading security concern, whether due to inadequate data security policies, non-adherence to existing policies, intentional malicious acts, or even the increasing shift to BYOD.

IoT success hinges on trust, making privacy another major issue. What data is captured and stored? How? Who owns it? How may it be used? How should and will it be protected through its use cycle, and by whom?

While these challenges apply generally to IoT deployments, the Public Sector faces some truly unique and consequential situations. Consider the implications of generating data that precisely reveals the location of dismounted soldiers in combat, the specific timing and location of municipal buses en route, safe campus video monitoring, or public health threat information, to name just a few.

Given the enormous changes that IoT will eventually bring, Federal regulation and policy are inevitable but will remain unclear for some time, politics being what they are. State and municipal-level policies vary greatly. Policy needs to be appropriately aligned to possibility for each environment, but some formidable issues must be addressed first:

> **Data Collection.** Many public sector mission and business leaders want to collect data from untrusted sources that can facilitate better, faster decision-making, such as improving threat, health or environmental analysis. But many current cyber security policies conflict with data collection, limiting what can be captured. The pressure is on IT to open up, yet security can't be compromised.

What's Your Experience?

IDC claimed that 2014 would be a turning point for public administrations. The mandate for greater efficiency is colliding with the imperative of transforming to meet increasingly savvy constituents' demands for a better citizen experience[1]. The paradigm of "doing new with less" is driving priorities such as the evolution of smart cities, the role of the Internet of Things, Big Data, intelligence and predictive analytics.

Have you found 2014 to be a turning point?

Cyber Security. To date, the market has been served with a complexity of disparate point solutions, mostly focused on prevention. Defense will always be the priority goal, but with malwares proliferating at two per second (and accelerating), a 100% prevention strategy is simply not possible. Malicious actors need to be right only 1% of the time or less to permeate the firewall. Therefore, it's not only prudent but necessary to prepare for the full attack continuum—before, during and after. An appropriate solution requires layers of security that span prevention, halting an attack in progress, and accelerating remediation after it occurs.

Bandwidth will always be limited, but data volume is only growing, with much of it useless—driving the need for edge-based data analytics to ensure the flow of just the most relevant data to those who will make use of it. Policy must guide what is considered most important and relevant, and who needs to receive what level of information.

Cloud. Not surprisingly, as adoption of cloud-based services increases, incidents of cyber-attacks on cloud environments are now nearly on par with attacks of on-premise equipment[1]. IoT connectivity will force a growing intersection of domains in the cloud environment: sensors and networks, IaaS and SaaS, Big Data analytics—yielding an increasingly expanded and vulnerable enterprise environment. Persistent security enforcement and information management policies are needed, where responsibility is shared between the service provider and the customer, to protect the data and the devices and people connected to it.

What then must CIOs consider when preparing for Trusted IoT deployment?

Given these challenging issues, Public Sector CIOs should lay some important groundwork when embarking on their IoT journey:

- Carefully plan the number and scope of initial IoT deployments that an organization can afford to undertake, including the investment in the needed people and skills, applications, analytics technologies and risk mitigation required to capitalize on the opportunity value: IaaS/SaaS, cyber security and Big Data. In an era of ridiculously tight budgets, existing infrastructure must obviously be leveraged as much as possible.

- Establish and maintain trust throughout the data lifecycle. Consider solutions like Suite B encryption (devised by the NSA), which secures data out to the tactical edge. Reliable firewalls between cloud and fog network nodes are also needed. Beyond the technology, only capture data that is truly needed for the business or mission purpose, then be transparent with citizens and stakeholders. Let them know what is collected, why, how it's used, and how it's managed and protected. Provide easy opt-outs when possible.

- Prepare for the full attack continuum. Design a robust security platform rather than approaching security from a point-to-point perspective. A combined hardware and software platform managing the connection, the applications, the devices and the data will enable CIOs to more readily enforce security policies and provide for security persistency. Correctly applied analytics can identify an attack in progress and help to remediate damage more quickly, but this approach will require intelligent information stewardship along with tight security.

- Educate the workforce. Push security messages frequently. Set reasonable access and geo-fencing policies that balance the desire for expanded data collection with the need for security, then enforce them as much as possible. Revisit them annually to assess and accommodate changing stakeholder requirements.

- Explore innovation partnerships with the private sector to create technical and policy solutions to IoT challenges. Feasible solutions can later be adopted cross-domain to maximize the potential benefits.

The Internet of Things has the potential for sweeping disruption, perhaps on par with only a few milestones in recent history such as World War One and the Industrial Revolution. While IoT may forever change the way public sector leaders protect and serve, trust is paramount to IoT success. Constituent participation will be weighed as a trade-off for utility received, such as a better citizen experience or increased public safety. Thoughtful, holistic planning should include not just the technological, but the fiduciary, legal and ethical aspects that will engender trust and drive to the greatest public good.

Kathy Stershic is Principal Consultant of Dialog Research & Communications, a consulting firm serving IT Executives through thought leadership messaging and informed, strategic communications planning. kstershic@dialogrc.com; blogging@dialogrc.com; @kstershic

[1] 2014 Cloud Security Report, Alert Logic http://www.computerweekly.com/news/2240219265/Cyber-attacks-move-to-cloud-with-adoption-report-shows