Campus IoT Briefing Doc

The Academic Enterprise and IoT: Opportunities and risks abound

The relationship between the academic enterprise and the Internet of Things (IoT) is particularly complex. For the research community, things are becoming a strategic academic advantage, for researchers developing the engineering of things, to researchers across many domains leveraging things for their own domain science. cutting-edge things. Operational units on campus are deploying intelligent devices to realize significant economic efficiencies, improve public safety, and provide a campus experience to a global community. Connected things are becoming core infrastructure. All of this is set against a backdrop where at most institutions, things are now connecting to the campus networks at far greater rates than people. And industry projections are that we are in the early stages of IoT growth, and ubiquity of devices and sensors being on net.

Yet at the same time great risks for institution and individual also abound. A couple of scenarios of risk:

Ransomware on a critical thing or service.

Departmental acquisitions clashing with other departments *<<JD: Architecturally, Spectrum, capacity and bandwidth impact = true cost increase to the institution>>*

Patching medically implanted devices *<<JD: Lack of standards, Threat to life-health-safety>>*

Other stories *<<JD: Massive growth trend, pivot point and identity vulnerabilities, introducing new vulnerabilities and threat scenarios, often outdated or insecure technologies, impact on compliance (particularly on assurance and attestation), compatibility forcing infrastructure re-work, undermines frameworks and best-practice standards (thus assurance), safety impact of sensor space (nature of many IoT devices to sense, provide alerts /security warnings such as freezer monitors, ICS/SCADA, etc.) >>*

<<JD: Primary motivational risk - Reputation impacting events create negative publicity, compliance situations hampering growth/strategic plans, limiting research opportunities and introducing fines and new compliance monitoring impact (e.g. HIPAA reporting for 20 years), or discouraging advancement and recruitment (High opportunity, moderate impact). Secondary from a lower opportunity standpoint, impact to life, health, and safety of devices in sensory, communications, transportation, or environmental monitoring situations. (Low to moderate opportunity, High to extremely high impact including constituent or visitor death.) The third most relevant might be the potential to undermine or undo compliance programs or frameworks by the introduction of the new devices/architecture - making attestations false. (Low to moderate opportunity, moderate to high impact)>>

There are several important lessons to be learned.

Pay attention, first and foremost. Both the institutional risk and reward warrant an enterprise-wide review process and management approach. Many universities have major exposures or are limiting the benefits that new technology can provide.

The risks range across a spectrum of reputational, financial, legal and security (availability, confidentiality, integrity, etc) vulnerabilities.

It is likely that gaps exist which result in significant institutional risk. Gaps in management of responsibilities, in the acquisition model, etc. A RACI framework may be a useful way for an institution to identify gaps and initiate processes and responsibilities. *<<JD: Clarifying accountability and responsibilities, not for the sake of heavy handedness and bureaucracy, but to promote good decision making and distributing the load. Don't let community think it is a central IT problem if that is not where you choose to invest in controls. Hold folks accountable for actions when problems arise, not interrupting strategic services and priorities. Defining and reinforcing highly critical and confidential/private standards and responsibility differentiation. There is an inherent central IT monitoring requirement regardless that must be funded if central IT has any role in compliance standards. >>*

Only so much can be managed. There are a lot horses out of the barn already, deployed as critical infrastructure in the institution. Moreover, the marketplace offers limited solutions.

It is not clear where or how to manage IoT. For example, asking the campus network organization to manage networking aspects of things may not be appropriate for cellular or Lo-wan connected devices.

There are new needs for data stewardship. Things generate data that can benefit or expose the institution. Who manages it? Most things put data in the cloud. Who owns that data?

One useful document may be a lifecycle-based checklist to help an institution have prudent acquisition requirements. Such a checklist is now under development by the Enterprise-IoT group at Internet2.