Some IoT Systems Vendor Management Considerations for Higher Education Institutions

Internet 2 CINO IoT Systems Risk Management Task Force
April 2017

To provide comments on this document, please email CINO@Internet2.edu

Purpose of Document

This document is intended to provide different organizations within Higher Education institutions with items to consider as they engage with IoT Systems vendors at the different phases of selection, procurement, deployment, and management. For example, these items/talking points can be used within the RFI, RFP, procurement, contract negotiation, deployment, and management stages. Different organizations within an institution will have different interests in the process and some organizations will have intersecting/overlapping interests with other institutional organizations.

It is acknowledged that IoT Systems are selected, acquired and deployed by Higher Education Institutions through multiple paths. Systems may arrive through PI's (Principal Investigators and their labs), through planning and budgeting departments, facilities management groups, capital development organizations, central IT, distributed IT groups, and multiple vendors and subcontractors.

The more historical acquisition approach of selection, acquisition, deployment, and management of traditional enterprise IT systems through central IT is not sufficient for doing the same with IoT Systems. Further, while IoT Systems will likely use IT infrastructure, such as wired and wireless networking, deployed and supported by central IT, to support the newly acquired IoT System, it is very likely that central IT will not have the resources or expertise to support the wide-ranging performance aspects required of the IoT System.

IoT Systems are unique in that they span many organizations, such as those mentioned above, within an institution. ***They are also unique in that they affect many types of risk within an institution*** to include financial, reputation, operational, safety and other types of risk.

For each of the statements or questions below for use in managing vendor relationships, ***two additional columns are provided: one for type(s) of risk involved and one for example organizations on campus*** that may be interested in the particular statement or

question at hand. In both cases – risk type and organization -- it is acknowledged that there can be overlap between types. For example, financial risk can also affect reputation risk. (Almost everything affects an institution's reputation risk). ***The risk item or the organization indicated are primarily intended to be used as examples and potential talking, negotiating, and management points.***

Example Higher Ed institutional organizations having interest include:

- Principal Investigator (PI) & lab staff
- Planning/budgeting office
- Capital development
- Facilities management
- Police department
- Central IT
- Distributed IT groups
- Risk, compliance, CISO, & privacy offices

Example Higher Ed risk areas include:

- Privacy
- Financial
- Operational
- Reputation
- Compliance
- Safety
- Cybersecurity

Both lists are not exhaustive and both lists have items that have interdependency on other items. The intention is to consider them in planning, talking, negotiation, and vendor management activities and to inform and elevate the conversation.

Issue/Statement/Question	Example potential risk area	Example institutional org having interest
● Does IoT vendor need 1 (or more) data feeds/data sharing from your organization? ○ Are the data feeds well-defined? ○ Do they exist already? ○ If not, who will create & support them? ○ Are there privacy considerations?	e.g. operational, CISO, privacy, …	e.g. Central IT, PI …
● How many endpoint devices will be installed? ○ Is there a patch plan? ○ Do you do the patching? ○ Who manages the plan, you or the vendor? ○ What is involved (labor / time) in a patch in relation to the scale of the IoT System	e.g. operational, financial, …	e.g. Facilities Mgmt., Central IT …
● Does this vendor's system have dependencies on other systems? ○ If so is that second system (and even subsequent dependencies) changing rapidly? ○ Is there a plan or resources to manage these interdependency integrations?	e.g. financial, operational, reputation, …	e.g. Central IT, Facilities Mgmt, Capital Dev …
● How many IoT systems are you already managing? ○ How many endpoints do you already have? ○ Are you anticipating/planning or planning more in the next 18 months?	e.g. financial, operational, reputation, …	e.g. Facilities Mgmt, Central IT, Capital Dev …
● Are you following a standard Dev / Test / Deploy process? Other?	e.g. operational, compliance …	e.g. Central IT, local IT, Facilities Mgmt …

● Is there a commissioning plan?	e.g. financial, compliance, cybersec …	e.g. Capital Dev, Facilities Mgmt …
● Have IoT vendor deliverable expectations been stated? ○ E.g. Contract, memorandum of understanding, letter, other? ○ How does the vendor manage security in the course of delivery? ■ Has the vendor changed default logins and passwords? ■ Has the password schema been shared with you? ■ Are non-required ports closed on all your deployed IoT endpoints? ■ Has the vendor port scanned (or similar) all deployed IoT endpoints after installation? ○ Is there a plan (for you or vendor) to periodically spot check configuration of endpoint devices? ○ Can you find suggestions on how to hack your IOTS from a Google search?	e.g. operational, financial, compliance, …	e.g. Central IT, CISO, Cap Dev, Facilities Mgmt, Planning/Budgeting …
● Has the installed system been documented? ○ Is there (at least) a simple architecture diagram? ■ Server configuration documented? ■ Endpoint IP addresses & ports indicated? ○ Does the documentation follow any sort of standard? Is it readable and consumable across multiple different parties?	e.g. reputation, operational	e.g. Capital Dev, Central IT, Facilities Mgmt, Compliance …
● Who pays for the vendor's system requirements (e.g. hardware, supporting software, networking, etc.?) ○ Does local support (staffing/FTE) exist to support the installation? Is it available? Will it remain available? ○ If supporting IoT servers are hosted in a data center, who pays those costs?	e.g. financial, operational, cybersec	e.g. Planning/budgeting, Facilities Mgmt, Central IT, PI/end-users …

■ startup & ongoing costs? ○ Same for cloud — if hosted in cloud, who pays those costs? ■ startup & ongoing costs? ■ Is your approach to cloud hosting based on standard server procedures or on customized services?		
● What is total operational cost after installation? ○ licensing costs ○ support contract costs ○ hosting requirements costs ○ business resiliency requirements costs ■ e.g. redundancy, recovery, etc. for OS, databases, apps	e.g. financial, operational, risk	e.g. Facilities Mgmt, Capital Dev, Planning/budgeting …
● How can the vendor demonstrate contract performance? ○ Okay to ask vendor to help you figure this out ○ Does the vendor's component include a readily engaged / checked self-test?	e.g. financial, cybersec	e.g. Facilities Mgmt, Capital Dev, Central IT, local IT …
● Who in your organization will manage the vendor contract for vendor performance? ○ Without person/team to do this, the contract won't get managed	e.g. financial, operational, cybersec, …	e.g. Planning/ budgeting, CISO, Risk …
● Can vendor maintenance contract offset local IT support shortages? ○ If not, then this might not be the deal you want	e.g. financial, operational, …	e.g. Facilities Mgmt, Central IT, Cap Dev …
● For remote support, how does vendor safeguard login & account information? ○ Do they have a company policy or Standard Operating Procedure that they can share with you?	e.g. cybersec, operational, safety …	e.g. CISO, Central IT, Facilities Mgmt …

● In cases where you are administrating access: Does the vendor maintain a back door?	e.g. cybersec, operational …	e.g. Central IT, CISO, Risk, Compliance …
● Is a risk sharing agreement in place between you and the vendor? ○ Who is liable for what?	e.g. compliance, financial, reputational	e.g. CISO, Risk, Facilities Mgmt, Central IT, …
● What standard of emergency resiliency should the system be built to? ○ Is there existing emergency power, cooling, if needed?	e.g. operational, reputation, financial …	e.g. Planning/budgeting, PI/end-user, Risk …
● Are there systems for which wireless connections are acceptable? ○ What criteria should be used to determine if appropriate?	e.g. cybersec, privacy, …	e.g. PI/end-user, Central IT, Facilities Mgmt. …
● How do we include requirements in a Design Guide? ○ What is the process for updating the guide? ○ How often? ○ Are there triggers other than time that lead to a revision?	e.g. operational, financial, compliance …	e.g. Capital Dev, Facilities Mgmt, Central IT, local IT …
● Does the System offer an event monitoring capability?	e.g. operational, cybersec, reputation …	e.g. Central IT (especially NOC), Facilities Mgmt, CISO, Risk …
● Is there a mechanism for integrating System-generated events with institution's existing ticketing system	e.g. operational …	e.g. central IT, Facilities Mgmt, local IT, …
● Does the System offer event trend analysis tools?	e.g. operational, financial …	e.g. central IT, Facilities Mgmt, …

● Does the vendor offer a proposed set of severity & urgency guidelines for Systems events	operational …	e.g. Central IT, Facilities Mgmt, …

Other Resources

- NIST Cybersecurity for IoT Program
  - https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf
- FTC & IoT Privacy
  - https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf
- Industrial Internet of Things Security Framework
  - http://www.iiconsortium.org/IISF.htm
- GSMA IoT Security Guidelines
  - http://www.gsma.com/connectedliving/future-iot-networks/iot-security-guidelines/
- OWASP IoT Security Guidance
  - https://www.owasp.org/index.php/IoT_Security_Guidance
- DHS Strategic Principles for Securing the Internet of Things
  - https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf
- Others …

Potential Future Work

- IoT Systems Costing
    - Few, if any, institutions have a handle on this
    - Vendor costs, local costs, total cost of ownership

- Network segment portfolio strategies
    - Segmentation is a popular concept, but how are those segmentation portfolios managed?

- Internal ICS & IoT exposure
    - Shodan/Censys do public addresses
        - Internal VLAN's, VRF's, etc. not covered

- Specific checklist for Network Operations Centers (NOCs)

- Benchmark/standard for exposure in HE

To provide comments on this document, please email CINO@Internet2.edu