The Internet of Things (IoT) and IoT systems have the potential to bring significant value to higher education institutions. Colleges and universities can benefit from IoT systems such as traditional building automation systems (e.g., HVAC), energy management and conservation systems, building and space access systems, environmental control systems for large research environments, academic learning systems, and safety systems for students, faculty, staff, and the public. However, without thoughtful implementation, that value will not be realized.
Quick Definitions
The Internet of Things consists of devices (i.e., “things”) that compute, are networked, and interact with the environment with the intention of collecting sensory data and/or manipulating the local environment. For example:

- A FitBit (http://www.fitbit.com/) computes, is networked, and interacts with the environment (i.e., collects data from the FitBit wearer).
- An industrial smart grid meter (https://www.smartgrid.gov/) computes, is networked, and interacts with the environment (i.e., collects power data).
- A residential Nest meter (https://nest.com/) computes, is networked, and interacts with the environment (i.e., collects temperature data).
- Devices in Chicago’s Array of Things compute, are networked, and interact with the environment (i.e., collect many environmental data points).
- Blood glucose monitors (https://www.accu-chek.com/us/) compute, are networked, and interact with the environment (i.e., collect data from the user).

An IoT system is a set of IoT devices that communicate with each other and/or communicate with a central server that aggregates data and/or provides control data.

Why IoT Systems Are Different
IoT systems are different from traditional IT and information management systems and require new approaches to achieve investment value as well as to maintain or enhance an institution’s risk profile. Five factors distinguish IoT systems from other technology systems: (1) the large number of devices; (2) the high variability of types of devices; (3) the lack of language and conceptual frameworks to discuss and easily categorize and classify devices; (4) the fact that they span many organizations within an institution; and (5) the fact that the hundreds or thousands of devices embedded in the physical infrastructure around us tend to be out of sight and out of mind.

Large Numbers
In 2011, Cisco predicted that 50 billion devices will be connected to the Internet by 2020, and the growth appears to be compounding. It can be difficult to wrap one’s head around the magnitude of this growth. To help, we can apply the old-school “Rule of 72” used in finance. The Rule of 72 was attributed to the Italian mathematician Luca Pacioli in the late 15th century, says that if a system is showing compounding growth (i.e., growing by a fixed percentage over multiple time periods), there is a quick method for estimating the time it will take for the initial value to double: divide the rate of growth (that steady percentage per time period) into the number 72. For example, if you buy a house that increases in value at 6% per year, the time it takes to double in value is approximately 72/6 = 12 years. To use an example in the IoT space, an International Data Corporation (IDC) report suggests an 18.6% annual growth rate in the IoT market in manufacturing operations, starting with a $42 billion market in 2013. Applying the Rule of 72: 72/18.6 = 3.9, meaning the market size will grow from $42 billion to $84 billion by 2017 (an estimated 4 years).

High Variability
The variety of types of devices and of the hardware and software components within each device is very high. IoT devices do numerous different tasks, including measuring building energy, video monitoring a space, reading a heart rate, and sensing air quality every few seconds in a research facility. Devices can have many different types of hardware from many different manufacturers as well as many different layers of software, each possibly from a different software company (or person). This huge variability contributes to the challenge of identifying device categories that can be helpful in developing risk management approaches.

Lack of Language
We do not have commonly accepted language or conceptual frameworks for talking about the IoT and these systems. Without a shared language, planning IoT systems implementations or managing risk around systems is very difficult. It is also challenging to establish standards and vendor contract performance expectations without this language.

Spanning Many Organizations
IoT systems tend to span multiple organizations within a higher education institution. For example, environmental control systems for large research spaces are...
rapidly increasing in number. These systems often sense and regulate air temperature, humidity, particulate levels, light, motion, and many other factors. These measurements are used for safety, energy efficiency, regulatory compliance, and other research needs. Implementing an environmental control system will likely involve an institution’s central IT organization, the facilities management group, the researcher/principal investigator, distributed/local IT organizations, and at least one and probably several vendors. Between these organizations are gaps through which systems accountability and ownership can fall. For example, the researcher thinks that the central IT organization is monitoring and managing the system and keeping it secure. At the same time, the central IT organization doesn’t know what is being plugged into the network backbone. Each one hopes the other is managing the system well. Because of this spanning nature of IoT systems, there is often no overarching visibility, much less ownership and accountability, for the whole system.

Out of Sight, Out of Mind
Finally, IoT systems are unique in that many of the technical parts of the IoT system—that is, the computing and networking endpoints—are built into the physical infrastructure, out of sight and out of mind. A smart grid or campus energy management system can easily have thousands of networking, computing, sensing endpoints that are built into campus buildings. We don’t think about them because we don’t see them.

Managing the Seam
One of the greatest areas of institutional risk related to the IoT does not necessarily come from the IoT systems themselves but, rather, from the implementation of IoT systems. A seam forms between the delivery of the system by the vendor/provider and the use of that system by the institution. Seams, in themselves, are not bad. In fact, they’re essential for complex systems. They connect and integrate various parts of a system, enabling it to work toward a cohesive whole. However, how an institution chooses to approach and manage these seams makes a significant difference.

Seams connect and integrate various parts of a system, enabling it to work toward a cohesive whole.

Taking a Snapshot of IoT Systems Exposure

There’s good news and bad news when it comes to getting a quick snapshot of an institution’s IoT systems exposure. The good news is that tools for doing this are publicly available. The bad news is that tools for doing this are publicly available. Anyone—those in higher education and those with malicious intent—can use the same tools. However, since those with malicious intent are most likely using their own, nonpublic approaches, these publicly available tools might well be a net benefit to higher education (if we use them).

Shodan (https://www.shodan.io/), a private endeavor, is the best-known of these public tools and has been around the longest. Censys (https://censys.io/), stemming from research at the University of Michigan and the University of Illinois at Urbana-Champaign, is the newer entry into the space. Although their approaches are different, the two tools do similar things: they scan (almost) all publicly available IP addresses, record the responses, and make the IP addresses, responses, and metadata (e.g., location data) available to the public. The scans look for devices often associated with IoT and traditional industrial control systems. Both tools have the ability to download data, and they offer APIs that allow direct access. So by using either or both tools and searching the IP address space of a campus, institutional IT leaders can get an idea of current exposure—results that can be surprising.
successful IoT system implementations and subsequent operation. In addition, the work and staffing required to manage these customer-to-vendor (and vendor-to-vendor) relationships and to provide the oversight needed to operate IoT systems safely and effectively often gets obfuscated by the promises and shininess of the new technology.

The implementations of IoT systems differ from traditional deployments of workstations, laptops, and servers. By their very nature, IoT systems have the ability to sense, record, transmit, and/or interact with the environments in which we live and work. Further complicating the IoT systems implementations and support is a factor noted above: these systems may well be invisible (out of sight, out of mind), meaning that the IT organization might not even know the systems exist, much less be able to provide central IT support.

Firms and institutions purchase IoT devices and systems en masse to address various needs in their operations. These IoT systems might be related to environmental control and energy efficiency, safety of staff and the public (e.g., fire, security), biometric authentication, surveillance, and other functions. As a result, IoT devices can be brought into an institution’s physical space and cyberspace by the hundreds or thousands or more. The partial or improper configuration of such systems and devices can lead to significant consequences for the institution—as can also a lack of planning regarding long-term support, whether local or via a vendor maintenance contract or both.

In most higher education institutions, implementing a third-party solution—hardware, software, SaaS, or hybrid—requires a supporting infrastructure for that solution. I call this supporting infrastructure a socket. The customer institution must create a socket that allows the vendor solution to interface with appropriate parts of the customer’s existing infrastructure. Taking the time and resources to plan, build, and maintain this socket is integral to the operational success of the new system. Doing so also provides the institution with an opportunity to manage some of the risk that the new system introduces.

One of the worst-case scenarios for an institution is believing that an IoT system seam is being managed when it actually is not. At this point in the evolution of IoT deployments, I suspect that this scenario is more often the rule than the exception. Successfully following the famed advice to “know yourself” can be elusive given the scale and speed of IoT innovation and growth and the lack of precedence for managing this sort of risk. The IoT phenomenon will undoubtedly change how we seek to know and characterize our higher education institutions and our IT organizations as a part of the risk management process. A good place to start knowing ourselves is planning, building, and managing that seam where the interesting things happen.

Vendor Strategy and Relationships

The vendor count for IoT systems being managed by an institution will only increase in the coming months and years and will likely increase substantially. Some of this increase will be from traditional systems like HVAC, which have been in the space longer than most and are maturing and extending their IoT development and deployment. Growth
in an institution’s vendor count will also come from companies with brand-new products and service lines made possible by IoT innovation and expansion. Many of the benefits of the IoT will result from products and services offered by vendors that interact and exchange information with each other, such as an IoT implementation leveraging the cloud. Regardless of the source, as the number of IoT vendors grows, the number of customer-to-vendor relationships will grow, and the number of vendor-to-vendor relationships will grow. A somewhat insidious side effect is that the number of relationships to be managed (or not managed) will grow even faster than the vendor count itself.

Every relationship has friction or loss from an idealized state. Nature has plenty of examples: pressure loss in a pipe, channel capacity limitations in information theory, restrictions in heat engine efficiency. The 19th-century Prussian general Carl von Clausewitz famously established the concept of friction in war in his book On War, in which he sometimes evokes the image of a match between two wrestlers. Relationships between business customers and vendors have friction too—from day-to-day relationship management overhead (e.g., communication planning and contract management) to more challenging aspects (e.g., expectation alignment/misalignment and resource allocation problems). Friction in a business relationship, which is unavoidable to some degree, means that less information gets communicated than expected and less work gets done in practice than in the idealized state. Both results increase uncertainty. Further, friction in a network of relationships can manifest itself in yet even more uncertainty.

With the increasing network of nodes (IoT systems vendors, in this case), the even-faster-growing number of relationships, and the friction that naturally exists, the business environments at our higher education institutions are becoming progressively complex. And all of this is accompanied by rising uncertainty. Thus, even though devising a strategy or policy around IoT systems deployment and IoT vendor management can be difficult to do, given the complexity and relative newness of the phenomenon, it is a vital task. But since we don’t know what is going to happen next in IoT innovation, how do we establish strategy? Also, the strategy might cost something in terms of technical framework and staffing—and that is particularly hard to sell internally. However, without some type of strategy or policy for an IoT system implementation, providers will offer the products or service line implementations that are best for them. This is natural in our market economy, but as business consumers, we need to be aware of this tendency and we need to manage for the greater good of our institutions.

The following are some useful questions to ask when establishing a strategy for IoT vendor relationships:

- Are there protocols that can be leveraged across multiple vendors? Does the vendor in consideration participate in open-source protocols?
- Does the vendor provide a mechanism to help in reviewing and managing its performance? If so, the vendor is acknowledging the additional complexity that managing many IoT systems brings.

Even though an IoT strategy or policy is almost guaranteed to be imperfect, incomplete, and ephemeral at this stage, the cost of not having one is much higher.

Socializing IoT Systems Risk

The IoT holds much promise, yet concerns regarding security, privacy, safety, and other issues are valid. Addressing this new source of risk involves several challenges. It’s easy for anyone to call out things that could happen with IoT growth: medical devices can be hacked, smart meters can be compromised to steal information, the utility grid has increasing exposure, drone videos are being intercepted and hacked. Long live fear, uncertainty, and doubt, right? Highlighting these issues is important, but the larger and more difficult task for an organization is to communicate risk around the IoT in a way that allows that risk to be managed.

Within an institution that already manages risk in some form, communicating and socializing the idea of IoT risk involves two broad components.
First, the IoT defies traditional classification/categorization and is still little understood. People have a hard time understanding the concept. To begin to manage IoT risk, institutional leaders must have some vocabulary for it. The IoT is still new, its effects are largely unknown and likely emergent, and its precedents and analogies are few. We need to surface some language and concepts so that it can be discussed.

Second, the other risks that the institution faces are still there: safety, liability, financial loss, reputation damage, technology challenges, business competition, and more remain. They haven't gone away just because the IoT showed up. We are asking senior leaders to make room in their list of existing risks to add yet more risk—perhaps substantially more. Nobody wants to hear this.

How we outline and explain these IoT security, privacy, and risk issues is thus critical. Since we are competing for a small slice of available cognitive bandwidth, we must use this opportunity to communicate as clearly as possible. Doing so could involve taking the following steps:

- Find out what other risks the institution is already grappling with.
- Identify places where the IoT and IoT systems are present currently in the institution or where they may be soon.
- Use the language of managing existing risk in the institution to begin to talk about managing IoT risk.
- Lather, rinse, repeat.

A key to this communication is to get some IoT systems risk concepts out now. Give leaders some language to use in reflecting on IoT systems risk and discussing it with their peers. It’s also important not to be heavy-handed in the approach. Yes, IoT systems risk is important, the dangers are potentially very high, and the opportunities for abuse are many, but the existing risks faced by an institution must be managed too.

**Where to Start**

Although the topic of IoT systems risk can seem overwhelming, there are mitigations that we can begin to apply now. Establishing an IoT systems vendor management plan (even if rudimentary), performing reviews of the institution’s public IP network space with tools such as Shodan or Censys, and identifying and developing institutional language to communicate IoT systems risk are all good places to start. Opportunities for improving the environment for IoT systems implementation in higher education include building common IT and information management “back-end” architectures for IoT systems and creating best practices for network segmentation approaches that support IoT systems.

The IoT and IoT systems have the potential to provide substantial value to higher education institutions. But the implementation of those systems creates seams within our existing IT and information management ecosystems. We will need to manage those seams in order to realize the full value of the Internet of Things.

**Notes**

5. The Internet2 Chief Innovation Office (CINO) recently launched an IoT Systems Risk Management Task Force to explore these issues and others and to identify areas for future work. See also the Viewpoints column in this issue of *EDUCAUSE Review*: Florence Hudson, “The Internet of Things Is Here.”

© 2016 Chuck Benson. The text of this article is licensed under the Creative Commons Attribution 4.0 International License.

Chuck Benson (cabenson@uw.edu) is assistant director for IT, facilities services, at the University of Washington. He serves as chair for the Internet2 IoT Systems Risk Management Task Force and chair for the UW-IT Service Management Board.