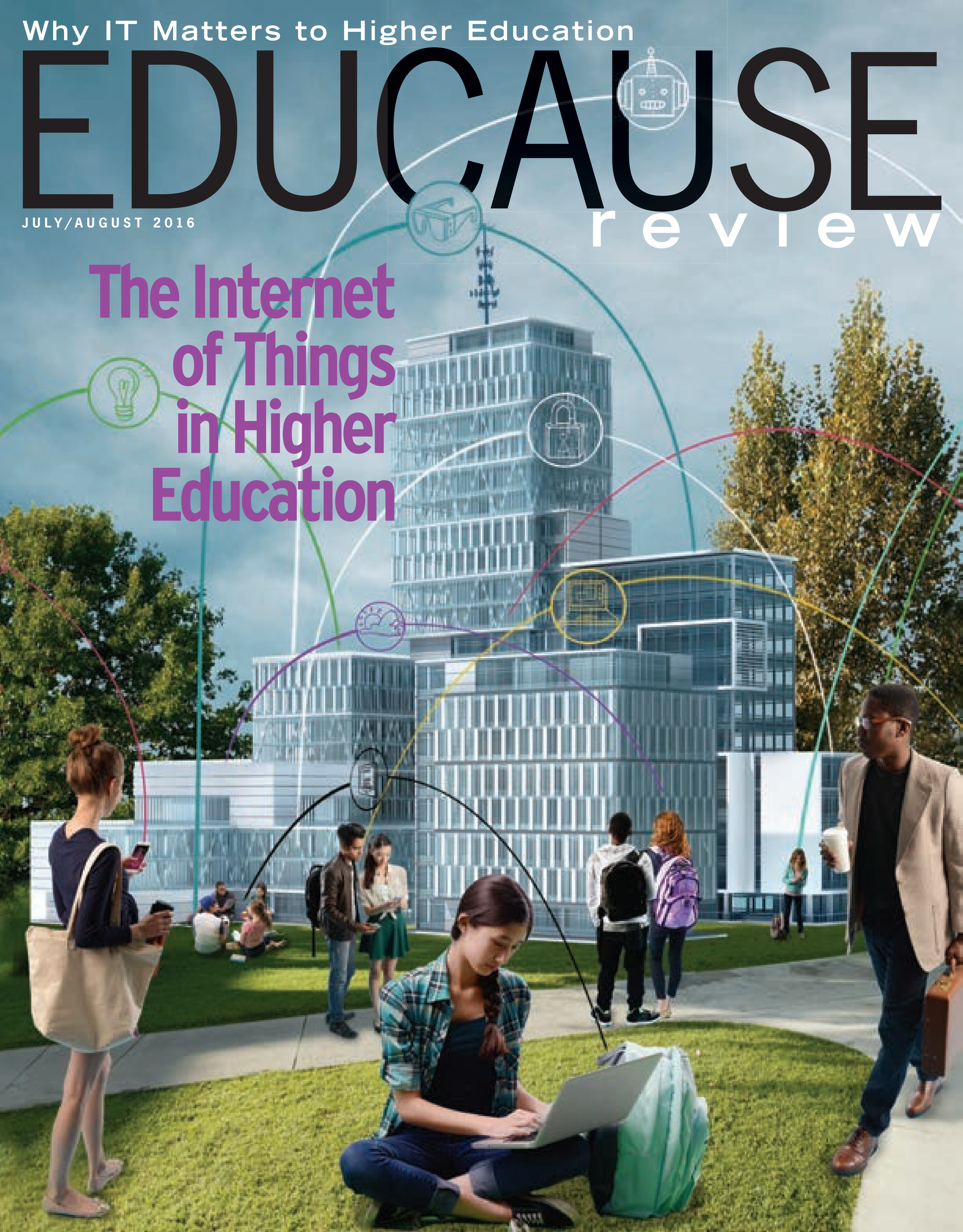
Why IT Matters to Higher Education

EDUCAUSE review

JULY/AUGUST 2016

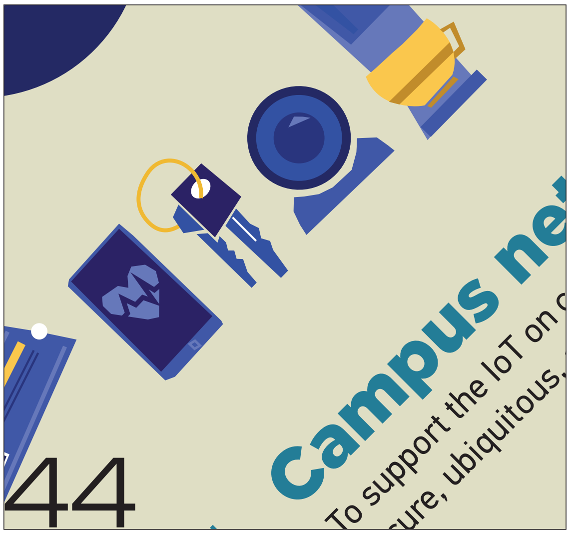
The Internet of Things in Higher Education




ONE SIZE
DOES NOT
FIT ALL

Why IT Matters to Higher Education
EDUCAUSE review
JULY/AUGUST 2016 VOLUME 51, NUMBER 4

FEATURES



Why IT Matters to Higher Education
EDUCAUSE review

JULY/AUGUST 2016 VOLUME 51, NUMBER 4

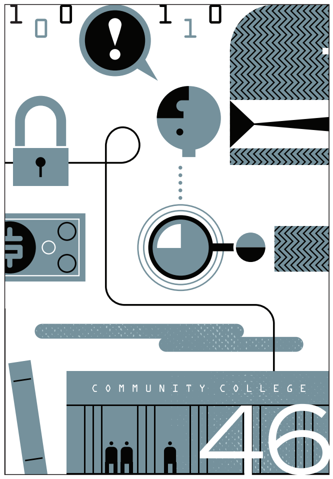
EDUCAUSE Review is the general-interest, bimonthly magazine published by EDUCAUSE. With a print publication base of 22,000, *EDUCAUSE Review* is sent to EDUCAUSE member representatives as well as to presidents/chancellors, senior academic and administrative leaders, non-IT staff, faculty in all disciplines, librarians, and corporations. It takes a broad look at current developments and trends in information technology, what these mean for higher education, and how they may affect the college/university as a whole.

282 Century Place, Suite 5000
Louisville, CO 80027
phone: 303-449-4430;
fax: 303-440-0461
info@educause.edu
http://www.educause.edu/

For subscription information, contact EDUCAUSE: 303-449-4430 (phone) or 303-440-0461 (fax) or <er-subs@educause.edu>. For advertising information, phone 720-406-6752, or fax 303-440-0461, or send e-mail to <advertising@educause.edu>. Send editorial submissions or comments to <editor@educause.edu>.

EDUCAUSE Review is also available online at <http://www.educause.edu/er/>.

COLUMNS



Volume 51, Number 4. *EDUCAUSE Review* (ISSN: 1527-6619) is published bimonthly (6 issues per year) by EDUCAUSE, 282 Century Place, Suite 5000, Louisville, CO 80027. Subscriptions are available at $48 per year ($78 per year outside North America) and to all academic libraries (North America and international) at $48 per year. Single copies are available for $10.00 each. Periodicals postage paid at Boulder, CO, and additional mailing offices. POSTMASTER: send address changes to EDUCAUSE, 282 Century Place, Suite 5000, Louisville, CO 80027.

Publications Mail Agreement #40033384
Return Undeliverable Canadian Addresses to:
Station A, PO Box 54
Windsor, ON N9A 6J5
e-mail: info@educause.edu

Cover: Ann Cutting

The next generation of Education Management has arrived

Fully integrated ERP, SIS and Research Management to help you:

- **Accelerate institutional growth** with powerful tools to increase productivity
- **Boost student success** by delivering on student expectations and needs
- **Improve institutional effectiveness** with reduced IT costs and intuitive reporting
- **Deliver research excellence** with improved project and funding management

Call or visit us today

1-888-247-3776

unit4.com/us/educause

UNIT4

In business for people.

By JOHN O'BRIEN

The Internet of Things: Unprecedented Collaboration Required

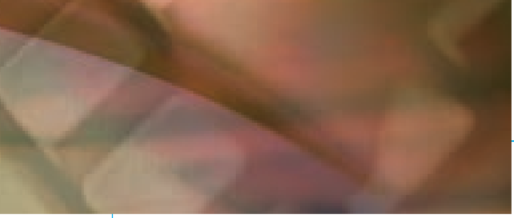
In this issue of *EDUCAUSE Review*, the predictions about the growth in the number of connected devices that make up the Internet of Things suggest a potentially dizzying pace of change. And it's a familiar story. In my last Homepage column, I shared the story of an editor who just barely caught herself before sending a thank-you note to a computer-generated assistant. The same week that issue of *EDUCAUSE Review* was published, a similar story broke in the higher ed IT world: most of the students in a computer class didn't know that their teaching assistant, "Jill Watson," was not a real person. In one telling statement, a student recounts that she grew suspicious because Jill Watson "responded so quickly."[1] Artificial intelligence services are maturing rapidly even while many of us are still trying to figure out how best to use Siri on our iPhones, and in this same way, the Internet of Things will surround us before we know it.

In "The Internet of Things: Riding the Wave in Higher Education," a panel of industry experts considers the speed, depth, and breadth of the IoT, paying specific attention to the potential impact in higher education. For example, TJ Costello, Director IoT for Cisco U.S. Public Sector, suggests that campuses might benefit from the innovations of "smart city" pioneers and recommends creating a "connected campuses" vision that can be accelerated by partnerships with industry. Bob Nilsson, Director of Solutions Marketing at Extreme Networks, envisions the IoT creating "dramatically improved" virtual classroom experiences for students taking classes from a distance. His evocation of "the images, the sounds, and even the smells" that can be conveyed by the IoT shows the sprawling vision for the higher education IoT. Some commentators focus on the IoT as activity monitoring—using smart lights, smart locks, smart HVAC systems, and other smart things. Likewise, fitness bands can gather data on students' pulse and body temperatures. Other commentators, like Nilsson, elaborate on the teaching and learning dimension. For instance, student brainwaves could even be measured to track cognitive activity during class. Maggie Johnson, Director of Education and University Relations at Google, is also excited by the IoT opportunities relative to teaching and learning and points to the "living lab" at Carnegie Mellon University and the promising academic research under way.

In their remarks, Chalapathy Neti, Vice President for Education Innovation at IBM, and Itai Asseo, Strategic Innovation Executive at Salesforce, include compelling observations about two themes that come up repeatedly in IoT discussions: (1) the vast amount of data and (2) the concomitant security and privacy risks. Neti goes so far as to suggest that whereas the 29 billion connected devices anticipated by 2020 (according to one estimate) will produce vast amounts of data, 90 percent of that data will not be visible to traditional computing systems. Of course, what happens to this data is of great interest to colleges and universities, which are already inundated by data in general and private personal information in particular. The potential for the IoT to dramatically improve living and learning on our campuses depends on our ability to analyze that data through an IoT platform. Neti sees great opportunities at the intersection of all this data and cognitive neuroscience, machine learning, and psychology. However, Neti also recognizes that "security is at the heart of IoT success."

Speaking to worries about security and privacy, Asseo underscores the connection between the IoT's attraction (functionality) and the IoT's detraction (privacy concerns), using the example of Disney World's MagicBand. The IoT functionality that allows people to tap their band and pay for things or make restaurant reservations at the resort generally outweighs its privacy detraction and thus seems "magical rather than creepy." This magic-creepy spectrum must be attended to as the IoT begins to materialize around us in higher education. "Having all the data about a user's information across different areas—to be used for personalization—brings up the risk of an experience that invades privacy and a certain personal space. That intrusiveness can be tolerated only if the value of that interaction exceeds the perceived cost of giving up some privacy."

The corporate panel discussion captures the vast complexity of opportunities and challenges related to the IoT. Chuck Benson, Assistant Director for IT, Facilities Services, at the University of Washington,

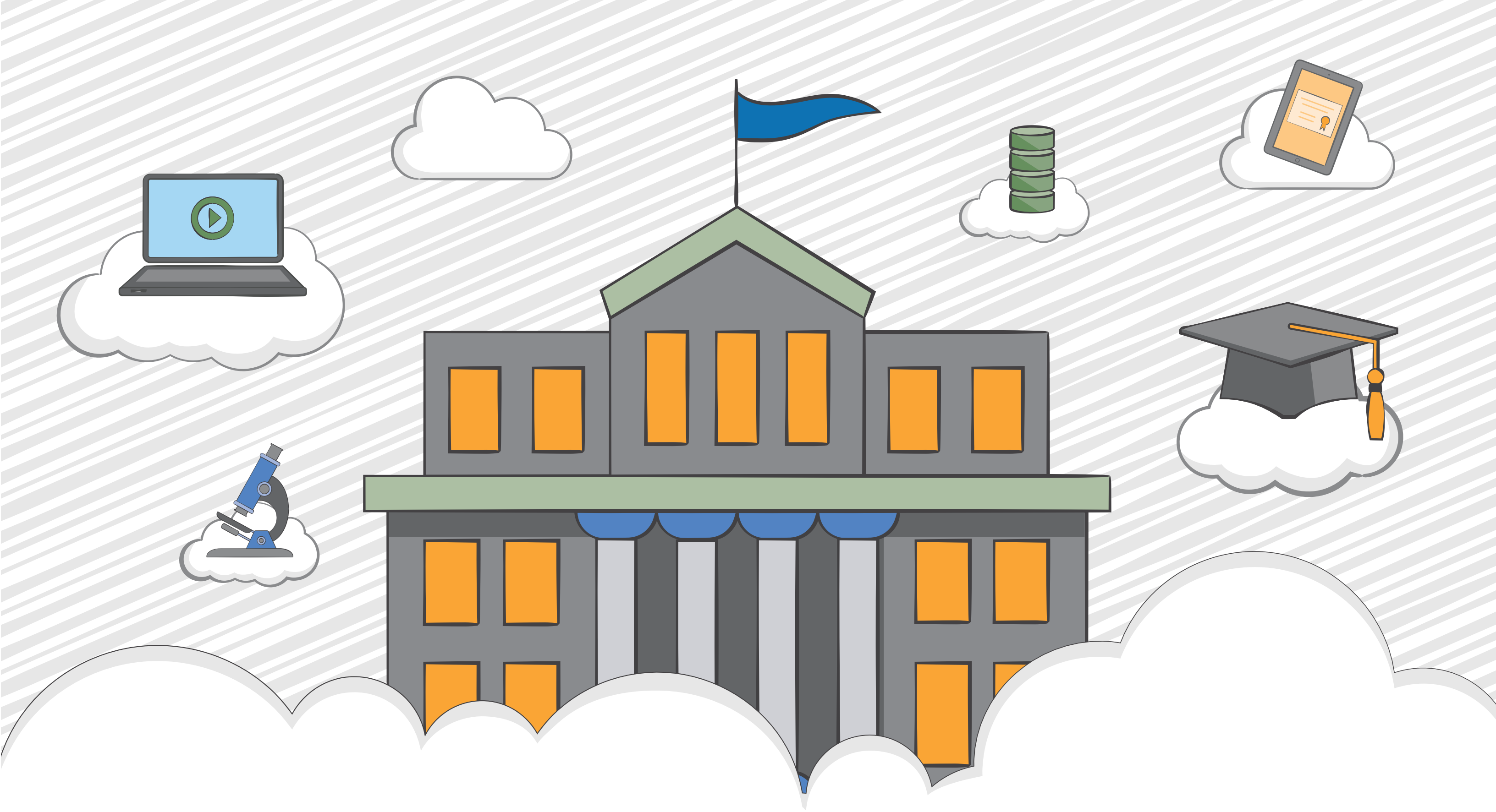


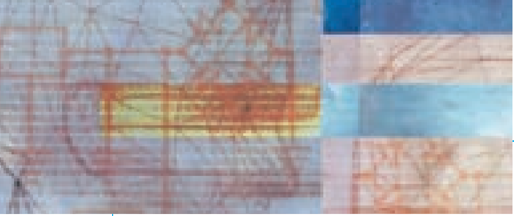
follows up with a concrete consideration of what the higher education community should be doing to ensure the thoughtful implementation that he sees as crucial to maximizing the benefits of the IoT and minimizing and managing the risk. Benson's analysis concentrates on five distinguishing factors of the IoT and on how campuses can and must develop new capabilities to deal with all that is new, especially related to vendor strategy and relationships. Benson acknowledges the difficulties at this early stage, pointing out: "Since we don't know what is going to happen next in IoT innovation, how do we establish strategy?" After suggesting directions, he stresses that even though any IoT strategy or policy developed at this early phase will necessarily be imperfect or incomplete, "the cost of not having one is much higher." Finally, Benson stresses the need to identify the risk around the IoT, to begin the important but challenging work of "socializing the idea of IoT risk," and to understand IoT risk in the context of other, already existing risks.

As the various voices in this issue of *EDUCAUSE Review* make clear, the challenge with the Internet of Things is not just the number of things but also the number of people and players. Higher education, living very much at the intersection between technology, people, and processes, can do much more than scan the horizon. In fact, in her Viewpoints column Florence Hudson, Senior Vice President and Chief Innovation Officer for Internet2, insists that "the higher education community can lead the development of the technologies, business models, ethics, and leaders of the IoT-enabled world." For the Internet of Things to add value to the world of higher education, unprecedented collaboration between all those involved—not just colleges and universities but also the industries that support higher education institutions—will be crucial in the sea change ahead.

Note

1. Melissa Korn, "Imagine Discovering That Your Teaching Assistant Really Is a Robot," *Wall Street Journal*, May 6, 2016.





Avoiding Failure with Higher Education Technology Projects

I am frequently asked for a definition of a "successful" technology project. As a career senior technology executive, university educator, and now university chief executive, I have a deceptively simple answer. A successful technology project is one that is delivered on time, that comes within budget, and that meets or exceeds stakeholders' expectations. Yet according to a study conducted by McKinsey & Company in collaboration with the University of Oxford: "On average, large IT projects run 45 percent over budget and 7 percent over time, while delivering 56 percent less value than predicted."[1] When I look around higher education, I would say these numbers are optimistic.

Why Higher Ed Technology Projects Fail

The easy answer to explain why technology projects in higher education fail is to place blame on ineffective project management and lack of communication. Technology project postmortems generally fail to get to the root causes of project failure—probably because true reflection means having to deal with the painful realization that the institution was ill-equipped to undertake the project in the first place. From nearly four decades of technology project-management experience, I see five main risk factors that lead to technology project failure. These risk factors are interrelated, and a failed project typically exhibits two or more of these factors.

From nearly four decades of technology project-management experience, I see five main risk factors that lead to technology project failure.

Inadequate or Incomplete Definition of Requirements

In this age of agile project management, we seem to have lost appreciation for having a requirements document that details such items as the purpose for the technology project (including financial ROI), mandatory and desired functionality, and data conversion and retention requirements. In essence, what are the institutional, functional, and/or programmatic outcomes that the technology project must achieve? These outcomes form the basis for a *project rubric*, which can be used to evaluate aspects such as competing technologies (or systems), mode of implementation (e.g., "build versus buy" or a local server-based solution versus a cloud-based one), conversion schemes, documentation, and training. Without this rubric, how does one know whether or not this technology project has a chance of succeeding?

Lack of Stakeholder Involvement

I cannot overemphasize the importance of stakeholder involvement in a technology project. All too often, the technology department of a college or university initiates a technology project—and obtains funding for it—without involving administration, faculty, staff, students, and others who will potentially be affected by the outcomes of the technology project. Collaboration and cooperation between stakeholders and the technology organization are keys to project success.

Two decades ago, I was engaged by a college to "rescue" a student information system (SIS) conversion that was late and over budget. It was in month eight of what was supposed to be a nine-month project, yet no academic or cocurricular departments knew anything about the project. They were not involved in the selection of the new system, were never scheduled for training, were never asked to validate the student data being converted, and were never included in any other aspect of the project. The technology organization's rationale for this lack of stakeholder involvement went something like this: "They are too busy to be involved. We will train them when the technology team is ready to deliver the new SIS."

In another, more recent SIS implementation, the institution's technology organization proceeded with a "dry conversion" from a legacy homegrown system to an integrated vendor-supplied system. Thirty months later, and eighteen months after "completing" the SIS implementation, the institution is still struggling with the new system. Why? Without stakeholder involvement up front and during the project, the new SIS was made to mimic inefficient workflows based on the legacy system, data interrelationships were not understood by the technology folks (resulting in numerous data-related issues), and stakeholders again received "just in time" training that was ineffective.

Unrealistic Schedule

Higher education is not alone in its tendency to set schedules at the top of the organization. Some schedules reflect the reasonable constraints of a semester or term systemfor example, upgrading computer lab equipment over spring break, implementing a new financial system based on the fiscal year, or deploying a new admissions system over a semester break. Fitting implementation into the first available break in the

By Norbert J. Kubilus

academic or operating schedule is not a valid reason to rush a technology project.

Many higher education administrators (like their counterparts in the private sector) are unfamiliar with what it takes to deliver a technology project, especially the time needed to perform data quality control and to train faculty and staff to a level of proficiency with the new technology. Yes, taking longer to correctly complete a technology project has an associated cost, but so does delivering one that is doomed to fail. As I used to tell my software engineering students: Spending $1 to catch and correct an issue in the requirements stage of a project will avoid the $1,000 that will be required if the issue is left undetected until after implementation.

Scope Creep and Inadequate Change Control

Without a project rubric, it is difficult to contain the scope of a technology project. With overactive stakeholder involvement, there is a tendency to add functions and features—or to turn on options—that at best are a marginal improvement to the system being delivered. The results are cost overruns, missed project deliverables, and schedule changes. Every technology project should have a formal change-control process to handle implementation realities *and* stakeholder requests. One reasonable way to deal with requested changes is to create a priority list of those requests that can be accommodated in the initial implementation and those that will come later.

Ineffective Documentation and Training

The project rubric should be the foundation for ensuring the adequacy and effectiveness of documentation and training. Vendor documentation and training should be examined for every function and feature listed in the project rubric; institution-developed documentation and training should emanate from the project rubric. It's never too early to start scheduling training for stakeholders based on their need to know or use the new technology. Here again, collaboration is essential.

Honing a Successful Technology Project Team

Mitigating project risk factors is a major part of avoiding technology project failures, but doing so will not be enough. A successful project requires strong project-management skills, frequent and clear communications with stakeholders, and a well-functioning project team. Honing a successful team to undertake a technology project requires preparation, leadership, and internal communication.

A technology project team brings together people who may or may not have worked together before. Some come from the technology organization, some are stakeholders, and still others are consultants or vendor representatives. It is extremely important that every member of the team knows his or her role and responsibilities and how to communicate within the team and has received an overview of the project itself, including goals, assumptions, limitations, constraints, deliverables, and deadlines. Conveying this information is the job of the project manager. Regardless of how many times these team members have worked together, this orientation is absolutely necessary.

Also key to preparing the project team is providing team members with the resources they will need to undertake the project—for example, hardware, software, Internet access, documentation, and training. Too often, higher education technology projects launch with insufficient resources, in part due to budgetary constraints. Time is another needed resource. Team members must have the dedicated release time necessary to spend on the project. This is extremely important for faculty and staff stakeholders, who will find it difficult to juggle project duties with everyday teaching or office responsibilities.

When a problem arises with the project—and it will—the team members and the project manager need to know about it and work together to get the project back on course. The project manager must anticipate problems, take corrective action, and help the team learn from the problems and issues encountered. Protecting the team from untoward external influence or pressure is also a key role for the project manager.

Continuous, positive reinforcement for team members can go a long way to moving the project forward successfully. There can be a lot of excitement and enjoyment in achieving the smallest of outcomes on a technology project. Acknowledgment of hitting project milestones helps build team morale, especially when the final deliverable is not yet in sight.

Takeaway

So what is the best way to avoid technology project failures in higher education?

- Have a strong project rubric based on stakeholder involvement. It will be the foundation for the project plan, documentation, and training, as well as ongoing communication with the stakeholders.
- Create a realistic schedule for the project and equip the project team with the necessary resources for success, including dedicated release time for this project.
- Commit stakeholder resources for testing and training.
- Empower the project manager to move the project forward without untoward pressure to change project scope or deliverables.

Finally, communicate ... communicate ... communicate! ■

Note

1. Michael Bloch, Sven Blumberg, and Jürgen Laartz, "Delivering Large-Scale IT Projects on Time, on Budget, and on Value," *McKinsey & Company*, October 2012.

Norbert J. Kubilus (nkubilus@coleman.edu) is president and CEO of Coleman University, a private nonprofit teaching university. Founded in 1963 and located in San Diego, California, Coleman University offers degree programs that prepare its graduates for technology-focused careers.

ILLUSTRATION BY ANN CUTTING, © 2016

THE INTERNET OF THINGS: Riding the Wave in Higher Education

Itai Asseo

Maggie Johnson

Bob Nilsson

Chalapathy Neti

TJ Costello

Looking at the vast ocean that is modern-day computing, we can see that major developments come in waves. The arrival of mainframe computers in the 1960s generated the first wave (one computer for many people), followed in the late 1970s by personal computers in the second wave (one computer for one person). In 1988, Mark Weiser presciently observed that computers embedded into everyday objects, objects all around us, were forming the third wave—what he called *ubiquitous computing* (many computers for one person). A decade later, in 1999, Keven Ashton put forth the ideas behind, and coined the term for, the fourth wave: *the Internet of Things.*

In this paradigm shift, Weiser's computer-embedded everyday objects—or "things"—are connected to the Internet and can communicate with users and with other devices. The guiding principle is *connection*, along with the conviction that if something *can* be connected, it *will* be connected. Indeed, in recent years, the wave appears to be rising to a crest. The plunging cost and size of processors and chipsets, the massive expansion of the IP address space, and the growing coverage of broadband networks allow virtually any object to be connected to the Internet. The computers, laptops, tablets, and smartphones that constitute the bulk of the Internet of Things (IoT) today are being joined by smartwatches, smart appliances, cars, lightbulbs, and an array of other devices that collect and transfer data, often without any human involvement. As that data is increasing and the technologies are advancing, we are moving from the early IoT of smart connections to a new phase, one of invisible integration.

Predictions for the growth of the IoT vary considerably: some experts forecast that about 20 billion devices will be connected by 2020; others put the number closer to 40 or 50 billion; and some even foresee as many as 100+ billion connected devices by that time. Regardless of the exact number of devices, spending in this market is expected to increase substantially, with the International Data Corporation (IDC) calculating that the worldwide market for IoT solutions will reach $7.1 trillion in four years. Clearly, the hardware, networking, software, analytics, and device/component vendors are embracing the IoT.[1]

What does all this mean for colleges and universities? Considering the key role being played by vendors in this market, we decided to ask some industry leaders in higher education a few questions. These experts have been looking toward and anticipating the IoT for quite some time, perhaps longer than many campus leaders and IT staff. In addition, they have valuable cross-industry insights to share with higher education. Who better to help us understand the impact of the IoT?

Below, five industry leaders give their perspectives on the IoT and new devices; the IoT benefits and campus influence; the problems solved/created by the IoT; and security, privacy, and data ownership issues. Based on their experiences with the IoT, they also share lessons learned and offer words of wisdom.

The Internet of Things is here. And it's big. Let's ride the wave.

Note

1. IDC, "The Internet of Things: Data from Embedded Systems Will Account for 10% of the Digital Universe by 2020," April 2014; Gill Press, "Internet of Things by the Numbers: Market Estimates and Forecasts," *Forbes Tech*, August 22, 2014; Gill Press, "Internet of Things (IoT) News Roundup: Onwards and Upwards to 30 Billion Connected Things," *Forbes Tech*, September 22, 2015.

The guiding principle is *connection*, along with the conviction that if something *can* be connected, it *will* be connected.

Itai Asseo

Strategic Innovation Executive
Salesforce

The Internet of Things has evolved over many decades as wearables, RFID, BYOD, wireless devices, and more have increased in both number and usage. How do you define the IoT today?

The *Internet of Things* is not a new term. It's been around since at least the late 1990s, but another decade or so went by before it became a mainstream term. The idea is that as computing power can be condensed into ever smaller units and devices, and as the power demand gets lower and more efficient, we can embed computing devices into anything from household items to clothing—and even into living matter.

That is the traditional view of the IoT. But as the IoT becomes more prevalent in our lives, we should be thinking about more than just the "things." The invisible part of this equation is the engine and the processes that enable these devices to be "smart." Most connected IoT devices can communicate simple data—for example, their location or a temperature reading of an object. But it is only *the connection of the device to an engine or database* that puts this data in context to other information. This is where we can truly unpack the value of the IoT. For example, perhaps the reading of the location and temperature are of a package containing important biological components for a lab, and the package needs to be shipped by a certain date and stay under a certain temperature. If any of these conditions aren't met, or are predicted to be unmet, a new delivery and alerts can be dispatched automatically. The IoT is all about moving from being reactive to being proactive and even being predictive as a result of automating processes and decision making.

> **"The IoT is all about moving from being reactive to being proactive and even being predictive as a result of automating processes and decision making."**

What game-changing IoT devices and uses do you expect we'll be seeing on campuses within the next one to three years?

We're already seeing some colleges and universities experiment with IoT approaches, such as adopting fitness devices to record student's health indicators or tracking temperature readings in lab equipment and sending notifications when certain conditions are met. But not all IoT solutions are going to come from extra devices, or "things." Many students and administrators are already carrying, every day, very powerful IoT devices in the form of mobile devices. In the next three years, we'll be seeing more campuses taking advantage of the current context in which students, administrators, and instructors operate. For example, by connecting a database of students' submitted work, students' schedules, and the time of day, the institution can send reminders and alerts when they are most effective, and each message can be personally tailored to the student. In addition, by employing some elements of gamification, the institution can reward students digitally for engaging and for completing tasks on time. To truly innovate, campuses need to combine information they gather from devices and from other sources in order to analyze and predict students' academic progress and identify problem areas and risk of attrition.

What are the most exciting academic and administrative benefits enabled by the IoT for higher education?

As we're already seeing in other fields such as media and marketing, one of the biggest potential benefits enabled by the IoT is a 1:1 journey that is personalized and unique to each student—from the recruiting and enrollment processes, in which communication can be tailored to who students are and the decisions they make, to the orientation process and ongoing engagement. Students can get personal recommendations on relevant academic topics/courses that they perhaps hadn't considered, events that might be of interest to them, and internship opportunities that could best suit their academic pursuits. When students' behavior indicates that they are struggling academically or personally, alerts can be sent so that administrators can reach out and act more quickly to resolve issues. In addition, students' profiles can be built over the length of their engagement with a campus, providing a better way for the institution to also assist them as alums, especially when coupled with employment activities post-academia. The truly exciting prospect of the IoT for higher education is that the more data we are able to capture about the different interactions that are happening continuously, the more we can improve practically every aspect of the institution's engagement with all parties involved. From the students' perspective, this interaction can become a significant factor when considering their options of where to spend their time and resources.

What higher education problems could be solved quickly with the widespread deployment of IoT technology? What problems might be created?

The IoT can help solve challenges across a wide array of topics, from logistics to administration to student life. So when designing an experience, institutional leaders should approach it first by discovering the biggest pain points. Streamlining and optimizing the utilization of facilities can help achieve financial savings (e.g., responding to weather events, automating operations). Smart devices can alert staff and providers about when to service equipment before a problem even presents itself. Smart doors, locks, and cameras can be used to monitor and control movement in different facilities. As more devices become connected, campus leaders will be able to extract much more value from the continuous stream of data and information, helping them move from a transactional relationship with students, faculty, administrators, and providers to an iterative process in which micro-decisions can be made on an ongoing basis.

Based on your experience with the IoT, what industry best practices or lessons learned do you think are significant to, and might apply in, higher education?

A great example of how the IoT is playing out in the real world today—an example that is applicable to higher education institutions—lies not in Silicon Valley but in Orlando, Florida. Disney World's MagicBand is a wearable device that transforms the entertainment experience into a much more personalized affair. The MagicBand allows guests to do everything from unlocking their rooms to making restaurant reservations to accessing the theme parks, and of course, to paying for anything in the resort—all simply by tapping their wrists. It's been a very successful implementation, but the main reason that the MagicBand works is that it exists in a closed environment where people enjoy having that extra bit of "magic." Whereas the same experience might come across as intrusive in other situations, in the contained environment of Disney World it seems magical rather than creepy.

What might a MagicBand look like in higher education? For students the academic experience becomes seamless, simple, and streamlined, with easy access to fitness/recreation facilities, academic buildings, residence halls, and athletic events and with simplified attendance, library access and lending, and payment at the cafeteria, bookstore, copiers, and more. Yet the real power comes into play for administrators and faculty. By leveraging the data of students' interaction with the campus at all times, higher education institutions can become more effective and productive as a result of mashing together different data points, such as attendance and performance, and can become more proactive, even more predictive, rather than reactive.

If you could offer a word of wisdom to higher education leaders on how to think about and apply the benefits of the IoT, what would that be?

The IoT benefits can be huge. If higher education fails to provide students with the advances and benefits of the IoT, students will look elsewhere. The key is to design student, faculty, and administrator experience that will have the highest value for all parties involved. Some of the most obvious advantages of having a connected campus also reveal some of the challenges. With any IoT user experience, the "creepy factor" spectrum needs to be considered. Two main areas that create this spectrum are personalization and transparency. Having all the data about a user's information across different areas—to be used for personalization—brings up the risk of an experience that invades privacy and a certain personal space. That intrusiveness can be tolerated only if the value of the interaction exceeds the perceived cost of giving up some privacy. On the other end of that spectrum, a lack of personalization can lead to less engagement and to an experience that feels "cold." Similarly, providing transparency to users about what data is collected, for what reasons, and from whom is extremely important. Finding out after the fact that certain information—personal or not—has been acquired without a user's knowledge can lead to mistrust. Yet when leveraged correctly, transparency can be used to create a sense of surprise and delight. ■

Maggie Johnson

Director of Education and University Relations
Google

The Internet of Things has evolved over many decades as wearables, RFID, BYOD, wireless devices, and more have increased in both number and usage. How do you define the IoT today?

At Google, we define the IoT as a network of everyday items with embedded computers that can connect directly or indirectly to the Internet. The number of devices connecting to the Internet is likely to grow exponentially over the next ten years.

What game-changing IoT devices and uses do you expect we'll be seeing on campuses within the next one to three years?

In addition to the enhanced educational experiences noted below, collaborative workspaces using projected or cast content can facilitate interactive group sessions for students and researchers. As these various interactions occur, massive amounts of data can be collected and processed using machine learning algorithms, which will allow for more personalized learning and accurate recommendations on what will further enhance a student's experience. All of these possibilities are enabled through the IoT.

> **"All IoT objects—such as thermostats, front door locks, and even cars—must have deeply ingrained, authority-based usage rights that carefully control access."**

What are the most exciting academic and administrative benefits enabled by the IoT for higher education?

The IoT is already present on most college and university campuses in the form of security cameras, temperature controls, and access to buildings, lights, power, etc. What's more interesting are potential benefits of increased connectivity that enhance teaching and learning or that provide new modes of operation. For example, ubiquitous access to computing power, high-quality online content, and social media and connections can be used to enhance the educational experience. Students can supplement their coursework with relevant video, activities, assessments, and conversations with students and faculty around the world. In addition, opportunities to do academic research on various aspects of the IoT are already under way in many higher education institutions—for example, the "living lab" at Carnegie Mellon University.[1]

How will the demands of a more connected student and a more connected campus influence—positively and/or negatively—the systems, processes, and infrastructure of the current higher education landscape?

New devices and the proliferation of smartphones and apps are generating huge amounts of data, which will continue to increase. It's no longer feasible to have that data processed in a central location. This will expand the complexity of the network and the potential for security holes—there's no such thing as a firewall with the IoT. These challenges are not unique to higher education institutions, but given the budget cuts and aging infrastructure in academia, the challenges may be more profound in that space. On the other hand, academic institutions looking for ways to conserve energy (and save money) can use energy monitoring and automation devices, allowing them to pay only for what they need instead of having to cool or heat large buildings whether or not the buildings are being used.

Will issues of privacy and data ownership stand in the way of a fully realized IoT? What other barriers or challenges will need to be addressed?

We believe there are three areas[2] that require significant investment and collaboration before an ecosystem can emerge to interconnect people, spaces, and institutions:

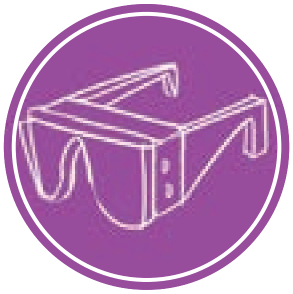
- Strong data management and identity controls must be built into the ecosystem from the start. All IoT objects—such as thermostats, front door locks, and even cars—must have deeply ingrained, authority-based usage rights that carefully control access. Users must also have control of their own data as it flows through this ecosystem. Regarding user control, in April 2016 Google added EIDs (Ephemeral Identifiers) to Eddystone, the Bluetooth low energy (BLE) beacon format we introduced last year. Since this beacon frame changes periodically, the signal is recognizable to only a controlled set of users, instead of being a public signal. We think EIDs will enable a new set of beacon use cases where users will be able to exchange information securely and privately.[3]
- The current IoT landscape is made up of individual solutions, or "walled gardens," that offer perks for customers who buy from a particular product family. If we are to learn from the development of the Internet, we know that the open ISP model provided superior services to customers. We need to find a way to do something similar for the IoT.
- Increasing the number of connected objects should not increase the screens or keyboards that we need for configuration or use. Technology should "fade into the background" via objects and services that provide real user benefit from connectivity and can be controlled through voice, gesture, or other relevant means of input. ■

Notes

1. Byron Spice, "CMU Leads Google Expedition to Create Technology for 'Internet of Things,'" *CMU News*, July 9, 2015.
2. See also Vint Cerf and Max Senge, "Taking the Internet to the Next Physical Level," *Computer* 49, no. 2 (February 2016).
3. Nirdhar Khazanie, "Growing Eddystone with Ephemeral Identifiers: A Privacy Aware and Secure Open Beacon Format," *Google Security Blog*, April 14, 2016.

Bob Nilsson

Director of Solutions Marketing
Extreme Networks



The Internet of Things has evolved over many decades as wearables, RFID, BYOD, wireless devices, and more have increased in both number and usage. How do you define the IoT today?

The phrase *Internet of Things* (IoT) generally refers to machine-to-machine (M2M) communications involving network-based remote sensors and actuators. Wireless sensors generate data (often "big data"), which can be stored and analyzed either on site or in the cloud. The range of smart IoT devices found in schools today includes e-books and tablets; sensors in hallways, entrances, classroom spaces, and campus vehicles; all sorts of fitness bands and wearables; virtual and augmented reality headsets; robots; video sensors; and smart displays, lights, and locks. Data from these devices can be used for simple tracking (e.g., campus shuttles, student attendance, and supplies) or for more complex monitoring (e.g., to understand student learning patterns as students progress through e-books and adaptive learning systems). Data can also be used for control. For example, the IoT provides the means to finely tune HVAC systems to keep all rooms throughout the campus optimally comfortable at minimum expense. Airflow, air quality, temperature, humidity, and lighting can be constantly optimized in every space that can conceivably be used for learning. Finally, flexible displays provide the important benefit of easily presenting data and status information on classroom screens or personal devices like smartphones and laptops. Modular dashboards and point-and-click control software (e.g., IFTTT, https://ifttt.com/) can easily configure sensors and actuators to create do-it-yourself, highly optimized custom-control systems. All of these IoT examples can ultimately enhance the learning experience for students and teachers, offering improved engagement and collaboration.

> **"The campus network is becoming a computational IoT nervous system, critical for keeping the facilities functioning and the learning environment alive."**

What game-changing IoT devices and uses do you expect we'll be seeing on campuses within the next one to three years?

I think we will see three categories of smart IoT-based breakthrough devices for the campus: remote-presence robots; virtual/augmented/mixed-reality headsets; and adaptive learning digital textbooks. The latter two in particular augur a new level of personalized learning. The adaptive learning devices can track how well individual students understand course content and can provide new content or offer supplemental teaching in various forms including video, text, experiments, or even virtual field trips.

What quantity of IoT devices would you anticipate having to support for the average student?

The number of different types of devices per student can be upward of five to ten. Starting with the smartphone, fitness tracker, tablet, laptop, and game device and adding jewelry like Ringly (https://ringly.com/) or Pebble (https://www.pebble.com/), nonportable devices like smart TVs, Wi-Fi lightbulbs, and Wi-Fi speakers for campus rooms, other small smart appliances, and a head-mounted display results in more than ten. Jon Bruner of O'Reilly Media notes how new breakthroughs in prototyping, fundraising, and manufacturing—collectively referred to as "the new hardware movement"—are opening a floodgate of Internet-ready, low-cost devices that students will want to take advantage of.[1] Although there is bound to be some bundling and consolidation of capabilities into single devices, the proliferation of new types of devices may more than make up for that.

What are the most exciting academic and administrative benefits enabled by the IoT for higher education?

One of the major academic benefits the IoT brings to higher education is a dramatically improved, higher-quality remote presence. Students who are unable to be physically present in the classroom can still experience the images, the sounds, and even the smells of the room.[2] Remote students can participate with the instructor and other students via remote-presence robotic devices such as Beam (https://suitabletech.com/getbeam/) and Double Robotics (http://www.doublerobotics.com/). Similarly, students no longer must be physically present in a laboratory to run science experiments. IoT devices such as TetraScience (http://www.tetrascience.com/) connect experiments and instruments to the Internet for control and monitoring from anywhere. PocketLab (http://www.thepocketlab.com/) and Lab4U (http://lab4u.co/) attach to smartphones to provide powerful, but still low-cost science lab instruments capable of measuring acceleration, force, angular velocity, magnetic field, pressure, altitude, and temperature. Combine these sensors with robotics and controllers, and online students are able to run, monitor, and directly participate in science experiments of all types.

A second benefit that the IoT brings to higher education is the ability to optimize the classroom learning environment. With the fine level of control and extensive sensor data available through the IoT, instructors can continuously adjust classroom conditions, which may be changed depending on the subject and the time of day. Both artificial and natural lighting intensity and even hue can be controlled. Air quality can be optimized, as can noise level. By monitoring the ambient sound level at the back of the room, instructors can be alerted if their voice becomes difficult to understand.

Student health and safety can be improved with wearables, video monitoring, and smoke, fire, and dangerous noise (e.g., gunshots) detection. Student engagement can be monitored to an extent well beyond simple automatic classroom attendance recording. The collective engagement of students in a classroom could be tracked by measuring changes in temperature, carbon dioxide, or the sounds of conversations. Students could be individually tracked via fitness bands that measure pulse rate, body temperature, and oxygen levels, and individual headbands (e.g., Muse, http://www.choosemuse.com/) could measure student brainwaves and pass along students' cognitive activities during class. Oral Roberts University integrated wearable technology with its physical fitness curriculum, though it quickly discovered the risk in terms of public perception.[3] Because the IoT provides rich data, it becomes possible to correlate all the conditions described above with student success to optimize the classroom and campus environment.

In terms of administrative benefits, the IoT enables more efficiency and therefore lower costs in facilities management. By remotely monitoring the HVAC, lighting, and almost everything that consumes energy and resources, institutions can optimize control. All inventories can be tracked and even automatically reordered when low. Safety can be improved with remotely monitored and controlled IoT locks. Outdoor campus lighting can be constantly optimized based on ambient levels, weather conditions, local activity, and anticipated patterns. Traffic can be eased with remote tracking and analysis. The instantaneous location of campus shuttles can be displayed on Google Maps, and school parking lots can be managed with smartphone apps. In addition, some students are hoping that colleges and universities use the IoT not only to improve safety and parking but also to reduce the price of tuition.[4]

How will the demands of a more connected student and a more connected campus influence—positively and/or negatively—the systems, processes, and infrastructure of the current higher education landscape?

The campus network is becoming a computational IoT nervous system, critical for keeping the facilities functioning and the learning environment alive. This nervous system thrives on solid, dependable, high-density, high-capacity, pervasive Wi-Fi. The need for wired networking at the edge is diminishing as almost all devices communicate wirelessly. The campus infrastructure must seamlessly handle roaming. IoT devices cannot disconnect and reconnect as they move about campus. Remote-presence robots become helpless without continuous Wi-Fi. Many mobile IoT devices reside inside of machines or enclosures and are inaccessible or are constantly in motion. Often the devices show up in locations where connectivity was not built in: HVAC mezzanines, closets, crawl spaces, elevators, fire staircases, and exits.

In its definition of the Internet of Things, the *Oxford English Dictionary* notes: "If one thing can prevent the Internet of Things from transforming the way we live and work, it will be a breakdown in security." Do you agree?

Security is definitely a concern, but if managed properly, it is not an insurmountable challenge. By employing adequate network-access control, rigorous network policy management, and network application visibility, colleges and universities can maintain security. Policies can help restrict what can connect to what, in order to guard against rogue devices and prevent interruption of critical flows of data and control. With these measures in place, institutions will be able to ensure that device control is permitted only from authorized points and that if an outside agent tries to either control a device or extract data, alarms will sound and the breach will be shut down.

Will issues of privacy and data ownership stand in the way of a fully realized IoT? What other barriers or challenges will need to be addressed?

As with BYOD, schools need a clear policy regarding what is allowed on the network in terms of both devices and data. Provision needs to be made to prevent overwhelming the network with streaming data and video. Just as some campuses now restrict Wi-Fi access to gaming consoles and bandwidth-consuming apps like Netflix, special provisions or restrictions may be appropriate for streaming IoT devices.

It is important to understand who owns the data that originates from IoT devices and that travels across the campus network. IoT product vendors assert a varying level of ownership over the software, the data, and even the products that an institution has purchased. Perhaps serving as a harbinger of these data, software, and product-ownership trends, the farm machinery manufacturer John Deere has asserted that the vehicle owner "receives an implied license for the life of the vehicle to operate the vehicle" but does not actually own the vehicle. Another example concerns digital environmental control systems in campus buildings. Is the data created by these systems owned by the HVAC system manufacturer, the real estate entity that owns the building, or the school that leases the space? Do the individual employees whose presence is monitored to optimize the lighting, heating, and cooling systems have rights to that data?

Higher education institutions should prepare for the following IoT-related regulation issues:

- Protecting IoT user and data privacy[5]
- Preserving patent rights for new combinations and mashups of IoT devices on the campus network
- Complying with licensing restrictions involving how a campus configures IoT devices and apps

Based on your experience with the IoT, what industry best practices or lessons learned do you think are significant to, and might apply in, higher education?

Historically, when devices similar to those associated with the IoT have come along, they have arrived suddenly and en masse. Think about the rapid growth of smartphones and game controllers; many IoT devices are even smaller and less expensive. IDC has projected that 200 billion devices will be capable of communication on the Internet by 2020 and estimates that 30 billion IoT devices will be connected by that time.[6] There have already been some IoT calamities. One example of what can happen when automated connections go awry was the trillion-dollar stock market "flash crash" in 2010.

Although the data demands of many of these devices start out lightweight, they grow as product vendors find how easy and low-cost it can be to add constant monitoring and even streaming HD

video to their devices. Since these are smart devices, they require periodic online software updates. Remember how networks seemed to go down whenever Apple released a new version of iOS? Imagine what could happen when thousands of IoT devices start requesting software updates during working hours. More consumer-grade products will also be used on the IoT. According to one recent survey, over half of education CIOs and IT managers are already evaluating consumer technology.[7] Higher education IT leaders need to be prepared to support the latest consumer IoT devices that are likely to show up on campus and need to be clear about which ones cannot be supported.

Effective technology roll-outs require three aspects: user training; adequate infrastructure, especially sufficient Wi-Fi coverage and bandwidth; and coordinated timing. Planning needs to be both defensive, ensuring that the IT infrastructure is ready and security concerns are met, and offensive, proactively encouraging and leading groups within and outside of the IT organization to take full advantage of the promise of the IoT. IT staff should have a solid understanding of the terminology, types of apps, and service-level agreements that will be required. To take full advantage of the IoT, however, institutions need to reach beyond the IT organization. For example, professors should understand how to incorporate the IoT into their curriculum to bring the subject matter alive, as well as to help students become comfortable with the technology, which will be an important factor in their professional lives.

If you could offer a word of wisdom to higher education leaders on how to think about and apply the benefits of the IoT, what would that be?

Get ahead of the flow of new IoT devices. Keep an eye on Kickstarter and Indiegogo for emerging IoT devices that may start showing up on campus, requiring campus network accommodations. Stay knowledgeable about the networking standards that may affect the IoT: IEEE 802.15.4 low-rate wireless personal area networks (LR-WPANs), IPv6 over low-power wireless personal area networks (6LoWPANs), BLE (Bluetooth Smart), and Wi-Fi HaLow. Informally or formally survey all campus departments to understand current and future IoT device use. Start planning institution-wide training. Undertake a pilot IoT project (see sidebar). Get all department heads involved in brainstorming new IoT-related educational opportunities.

Take advantage of the opportunity and responsibility to teach students how to design IoT products and systems. Incorporate new subjects in order to provide the skills that are necessary in an IoT business world, where analysis of big data from IoT sensors will take on a major role. Teach the base modules of the IoT (e.g., Arduino and Raspberry Pi). Most important, inspire creativity to apply the IoT to new businesses and concepts, and instill a vision of where the IoT can lead. ■

Pilot Internet of Things Projects

To set up a pilot IoT project on campus, start with something small that touches all the bases: sensors, controllers, security, data analysis, and reporting. Here are some simple ideas:

- Install IoT sensors on doors. Wi-Fi wireless door locks can pose challenges when rolled out en masse but are manageable as a pilot project tied in with other sensors, especially when limited to a few interior doors.
- Set up interior environment monitoring and control using Wi-Fi temperature and light sensors to track how well the HVAC system is performing and even how it correlates to student engagement.
- Program selected classroom or common space lighting (e.g., with Philips Hue or Hue Lux) to vary lighting over the course of the day (dimming bulbs when natural lighting is strong) and simulate clouds passing over. Track the results.
- Monitor activity at a receiving dock or movement in a lobby.
- Put Wi-Fi moisture IoT sensors in office plant pots to provide an alert when plants need watering.

Notes

1. Jon Bruner, "How the New Hardware Movement Is Even Bigger than the Internet of Things," *O'Reilly Radar*, June 4, 2015.
2. Liz Stinson, "This Magical Scent-Sending Phone Is Now Available to Order," *Wired*, June 16, 2014.
3. "Oral Roberts University Integrates Wearable Technology with Physical Fitness Curriculum for Incoming Students," *ORU News*, January 4, 2016; Stephanie McNeal, "People Are Furious at This College for Making Its Freshmen Wear Fitbits," *BuzzFeed News*, April 17, 2016.
4. Christen Palange, "3 IoT Advancements This Student Is Ready For," *Extreme Networks*, January 15, 2016.
5. Enza Iannopollo, "CIOs: Drive Internet-of-Things Strategies Forward with Effective Data Protection Practices" (Forrester Research report, May 13, 2015), includes an IoT data-protection checklist for CIOs, whereas *Internet of Things: Privacy and Security in a Connected World* (FTC Staff Report, January 2015) suggests the need for new cloud data-privacy regulations.
6. IDC, "The Internet of Things."
7. Bob Nilsson, "Here's How Innovators Stay Innovative," *Extreme Networks Blog*, March 18, 2016.

Samsung Wi-Fi

Blazing fast, high capacity Wi-Fi designed to power the communications and multimedia needs of schools today and tomorrow.

Carrier-Grade Wi-Fi | Smart Boards | Surveillance | Computers | Tablets | Smartphones

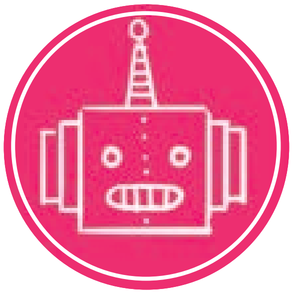
Contact us
www.samsung.com/wlan

Follow us
youtube.com/samsungbizusa
@SamsungBizUSA

SAMSUNG

Chalapathy Neti

Vice President, Education Innovation
IBM



The Internet of Things has evolved over many decades as wearables, RFID, BYOD, wireless devices, and more have increased in both number and usage. How do you define the IoT today?

The IoT is changing everything—from the way we drive, make purchases, and obtain medical treatment, to how we get energy for our homes. Data is emanating from everywhere. IDC predicts that by 2020, there will be close to 30 billion connected devices.[1] Today we define the IoT not only by its ability to connect devices (vehicles, buildings, wearables, and more) to a digital network, but also by its ability to directly integrate the physical world into computer-based systems. It is how people interact with this network of things that has become most interesting as the IoT has evolved.

Within two years, the IoT will be the single greatest source of data on the planet, but nearly 90 percent of that data will be "invisible" to traditional computing systems. This is where cognitive computing—such as IBM Watson (http://www.ibm.com/smarterplanet/us/en/ibmwatson/)—comes in. Cognitive computing can process massive amounts of data from a full spectrum of sources and can help businesses makes sense of and act on that data. Cognitive computing is enabling businesses to take full advantage of this burgeoning resource—data—while allowing systems to learn at scale, reason with purpose, and interact with humans naturally.

> **“Within two years, the IoT will be the single greatest source of data on the planet, but nearly 90 percent of that data will be invisible to traditional computing systems.”**

Today's IoT can fundamentally transform the way we interact with our surroundings. Because we can electronically monitor and manage a growing number of physical objects, we can now bring data-driven decision making to new heights of effectiveness. This helps businesses and people save time, be more efficient, and improve quality of life.

What game-changing IoT devices and uses do you expect we'll be seeing on campuses within the next one to three years?

Augmented Reality (AR) devices will be the next big thing. AR is poised to transform everything from games to art to education. We've spent our whole lives interacting with 2D media (e.g., paper, blackboards, screens, phones), but AR forces us to rethink everything we know about human-computer interaction. AR has the potential to truly revolutionize education. No longer confined by the limitations of a physical classroom, education can become so much more than lectures and tests.

AR will offer powerful contextual, on-site learning experiences and also serendipitous exploration of the connected nature of information in the real world. Now that the technologies making AR possible are much more powerful than ever before and are compact enough to deliver AR experiences to academic venues through personal computers and mobile devices, educational approaches using AR technology are more feasible. AR can make complicated mechanisms understood via contextually enriched interaction. For example, mechanical engineering students can study a 3D model of a camshaft arrangement in conjunction with a set of actual engineering components.

What are the most exciting academic and administrative benefits enabled by the IoT for higher education?

As more data is captured from billions of connected devices, and as new sources of data, such as social, become available, the potential for actionable intelligence increases exponentially. This poses tremendous opportunities for higher education. For example, it can help administrators understand their students better and help optimize the resources available to each of the students individually—everything from how crowded a classroom is to how often campus buses pass a specific location.

In addition, the IoT ingests data from a wide variety of sources inside a building—sources including sensors, meters, and lighting, and new sources such as weather and people presence—to help building managers act on data to enable "smarter buildings." For example, building managers can better understand which classrooms are used most often during "peak hours" and can better determine which lecture halls, residence halls, and facilities are most in need of technology upgrades.

How will the demands of a more connected student and a more connected campus influence—positively and/or negatively—the systems, processes, and infrastructure of the current higher education landscape?

A more connected student on a more connected campus can make a big difference to the current educational landscape. Think of mobile apps and crowdsourcing: similar to Waze, an app that recommends the most efficient driving route using real-time crowdsourced data, the process of learning consists of a series of tasks designed to get a student from competence state A to competence state B. Equipping learning facilities and students with IoT devices that monitor data, such as engagement and even emotion, can enable a more contextual, personalized, and adaptive approach to education—a Waze-like recommendation based on data pulled from many sources. Network-connected wearable sensors (NCS)—such as EEG, GPS, and VR—provide deep insights into the learner state, including how effectively he or she is learning. This can be used to provide real-time recommendations for improving learning outcomes based on similar learners' outcomes mined through crowd-sourcing. Evidence-driven insights—such as subject mastery, productivity schedule, and motivation index—can be assessed in real time to provide students with personalized learning recommendations that span their individual learning objectives, their courses, and their overall degree program.

What higher education problems could be solved quickly with the widespread deployment of IoT technology? What problems might be created?

IoT technology has the potential to improve operational efficiencies, connectivity, and collaboration. Seasonal campus services, such as registration and enrollment time, are examples of how higher education institutions could benefit from IoT deployment. Understanding the flows of use of various facilities during peak periods, campus buildings can allow for a more intelligent delivery of services. The IoT helps campuses to monitor and act in real time on that infrastructure.

Energy usage and space utilization are other areas where the IoT can help solve problems. Digitization is driving a growing convergence of the real world and virtual world, enabling institutions to leverage data analytics in the development of strategies to optimize energy efficiency and space utilization. With higher education institutions facing an ongoing challenge to reduce operating costs and get maximum use from existing space to support record numbers of students, these are serious issues that the widespread deployment of IoT technology could address.

IoT technologies, including smartphones and a Wi-Fi connection, are expected by students today, so campuses must be sure they have a quality IT and Telecom infrastructure to support that demand.

In its definition of the Internet of Things, the *Oxford English Dictionary* notes: "If one thing can prevent the Internet of Things from transforming the way we live and work, it will be a breakdown in security." Do you agree?

Security is at the heart of IoT success. That is why, as the number and the range of IoT devices grow on campus, it will be critical to ensure that communication between devices is secure. One way that higher education institutions can reduce their security risk is to build fine-grained perimeters to protect critical assets. The data is then assigned a sensitivity value, which helps protect it.

Right now, IBM Research is developing an *Enterprise Information Security Management* (EISM) platform, which aims to semiautomatically measure the sensitivity levels of enterprise assets, including both data and non-data assets. IBM Research is conducting pilot tests with a number of real-world cases, including scanning employees' laptops, classifying business documents, and ranking the sensitivity of servers without relying on data content. This approach has the potential to be applied to IoT devices in any type of enterprise, including educational institutions.

Based on your experience with the IoT, what industry best practices or lessons learned do you think are significant to, and might apply in, higher education?

Big data is arriving from multiple sources at an alarming velocity, volume, variety, and veracity. The data, by itself, does not generate any benefits: 90 percent of the data generated today is "dark" (unusable). To derive value from it, we need to connect all the data sources with a cognitive IoT system that can analyze it.

Unlike existing computers that must be programmed, cognitive systems like IBM Watson can learn at scale, can reason with purpose, and can interact with people naturally. Cognitive systems make sense of and give purpose to the collected data. Existing computers simply can't handle the volume and diversity of the data being generated everywhere, by everyone, every day. Cognitive systems, on the other hand, can properly utilize the data and can ensure that educational institutions are able to improve such core areas as learning experience, safety on campus, energy efficiency of buildings, and operational efficiency. But as part of utilizing IoT data, higher education institutions must ensure that the learner and the educator are fully opted in for any secondary use of the data collected from IoT devices.

If you could offer a word of wisdom to higher education leaders on how to think about and apply the benefits of the IoT, what would that be?

Both learning and teaching have benefited from integrating new technologies into the educational framework. However, integration by itself does not lead to a scalable, stress-free, adaptive, and personalized learning curriculum. Artificial intelligence and adaptive interactivity techniques need to be blended to achieve this. One promising approach for defining and monitoring the learning of an individual is to combine IoT and cognitive neuroscience research in the classroom of the future. The information that connected devices provide can be analyzed and, along with cognitive neuroscience, lead to deep insights into the brain's mechanism of learning and how it is being affected in a particular setup. In an era of adaptive, connected, and artificial intelligence, the combination of cognitive neuroscience, machine learning, and psychology will thus allow us to explore the science of learning and optimize future classrooms. ■

Note

1. IDC, "The Internet of Things."

TJ Costello

Director IoT
Cisco U.S. Public Sector

What are the most exciting academic and administrative benefits enabled by the IoT for higher education?
The IoT opens a range of possibilities and benefits for faculty, staff, and students. With the IoT, students are able to attend any class, at any time, from any device—providing them with greater flexibility to consume content and knowledge when and where they'd like. The IoT removes the traditional barriers to teaching and learning, providing faculty with the same flexibility to provide better learning experiences for students and allowing them to connect with experts from around the world and create robust, hybrid learning environments. The IoT also benefits administrators by helping to connect everything on campus everywhere through one secure, unified network to manage campus lighting, parking, HVAC systems, and cameras and to provide valuable data and analytics on traffic patterns, usage, and areas of resource optimization.

"Campuses can often be viewed like cities, and some of the greatest IoT innovations today are found in *smart cities*."

How will the demands of a more connected student and a more connected campus influence—positively and/or negatively—the systems, processes, and infrastructure of the current higher education landscape?
One of the biggest impacts of more connected students is when they come to campus with increased expectations about *experience*. Colleges and universities must reimagine the student experience, often by helping them to connect with previously unconnected systems. For example, can an institution tie a new student's location with the LMS to help the student get to his/her first class or to the right building for a study group? This requires that campus groups and departments collaborate to provide a better student experience and to ensure a solid, core infrastructure to support students' expectations and network demands. Campus leaders can look to retail stores and stadiums for ideas on how to deliver next-generation experiences.

What higher education problems could be solved quickly with the widespread deployment of IoT technology? What problems might be created?
The IoT presents a range of opportunities and challenges. One challenge is network security and physical safety. More connections to the Internet, with more sensors and other devices, create

access to the network from potential cybersecurity breaches. And physical safety can be one of the most important issues to a campus community. In fact, safety can be the reason a student might select a specific college or university. A variety of sensors, especially cameras, can now be completely integrated into a public safety system. This allows for quicker response times to an incident, making campuses safer. However, higher education institutions should also consider the policy implications of greater visibility into the lives of students and should be sure to balance privacy and safety. Including students in those policy discussions is one of the best practices that I have seen.

Based on your experience with the IoT, what industry best practices or lessons learned do you think are significant to, and might apply in, higher education?

Campuses can often be viewed like cities, and some of the greatest IoT innovations today are found in "smart cities." Leaders in this space have key goals for greater economic growth, reduced road congestion, and improved access to citizen services, very similar to the objectives of many colleges and universities. To achieve those goals, they have to work across all of the city's agencies, which can be a challenge. Often they create a new organizational structure or look to an independent third party to foster greater collaboration among different agencies. Higher education institutions can learn from leading smart city innovators: they can transform into fully connected campuses, or they can play the role of the independent third party to help enable smart city initiatives.

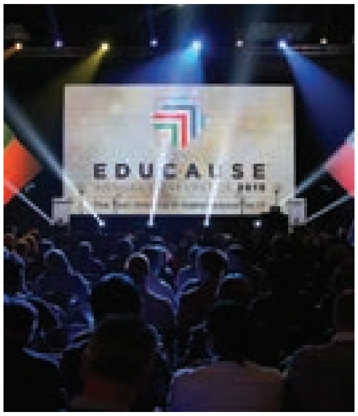
If you could offer a word of wisdom to higher education leaders on how to think about and apply the benefits of the IoT, what would that be?

The IoT can lead to breakthrough innovation and is creating entire new industries and new paradigms within existing industries. The best place to start is by having a vision of a fully connected campus to improve the experience for faculty, staff, and students. And the best way to help students is to consider your campus to be a living lab. Engage your students to help you innovate in solving challenges and creating opportunities. Bring in industry partners who can help accelerate innovation and also foster career opportunities for students. ■

7,000+
Participants

The keynote events were inspirational, the organization nearly flawless, the attendees are people worthy of networking with, the exhibits hosted vendors targeting education sector needs. Excellent job!

Great overview of all the technologies driving higher education.



EDUCAUSE

ANNUAL CONFERENCE **2016**

Sessions were very relevant to our campus needs.

1,200+
Institutions

Excellent presentations that covered a variety of topics that are relevant to me and my institution.

The Internet of Things, IoT Systems, and Higher Education

By Chuck Benson

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.

ILLUSTRATION BY SCOTT ROBERTS, © 2016

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).[1]
- 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.

IoT systems are different from traditional IT and information management systems and require new approaches.

Large Numbers

In 2011, Cisco predicted that 50 billion devices will be connected to the Internet by 2020,[2] 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, 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.[3] 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

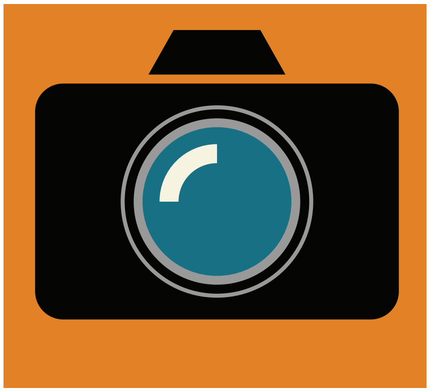
The variety of types of devices and of the hardware and software components within each device is very high. IoT devices do numerous different tasks, including measuring building energy, video monitoring a space, reading a heart rate, and sensing air quality every few seconds in a research facility. 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

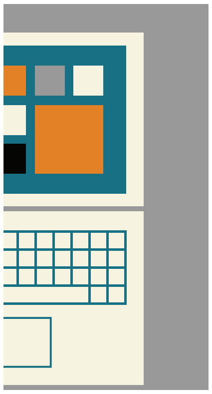
IoT systems tend to span multiple organizations within a higher education institution. For example, environmental control systems for large research spaces are



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 networked, computing, sensing endpoints that are built into campus buildings. We don't think about them because we don't see them.



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.

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.

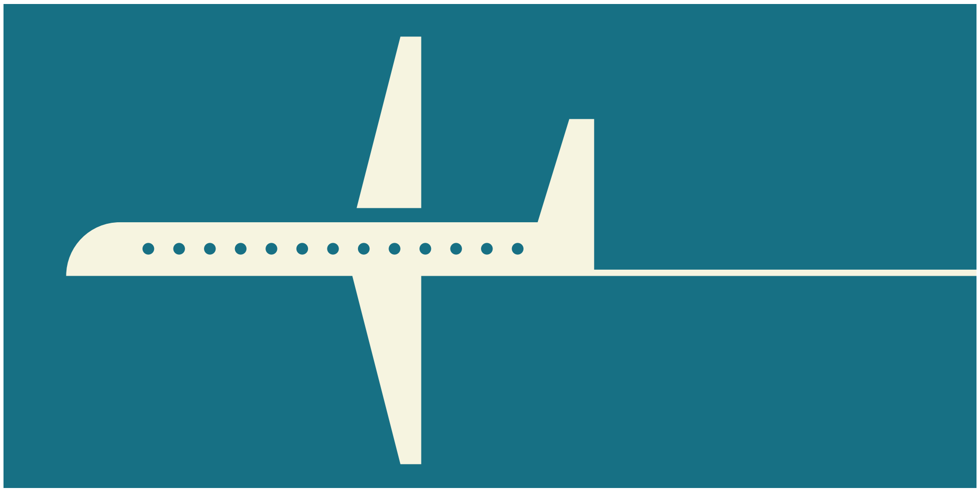
Seams are where interesting things happen. In 2015 college baseball changed its ball seams to flat instead of raised in order to drive more hits and home runs. Sure enough, both statistics increased.[4] In football seam routes, a receiver tries to exploit the gap between defenders. And anyone who has ever sat in the window seat by the wing of an airplane knows that there are many more seams in a plane than a passenger would probably care to see. Finally, seams can also be where things come apart.

Vendor relationships and vendor management have always been important for firms and institutions. However, the invasive nature of IoT systems makes vendor management particularly critical for

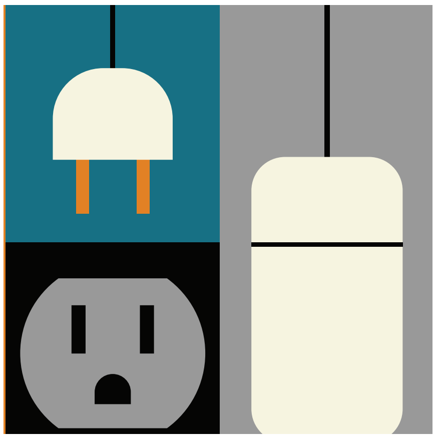
successful IoT system implementations and subsequent operation. In addition, the work and staffing required to manage these customer-to-vendor (and vendor-to-vendor) relationships and to provide the oversight needed to operate IoT systems safely and effectively often gets obfuscated by the promises and 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.



One of the worst-case scenarios for an institution is believing that an IoT system seam is being managed when it actually is not.

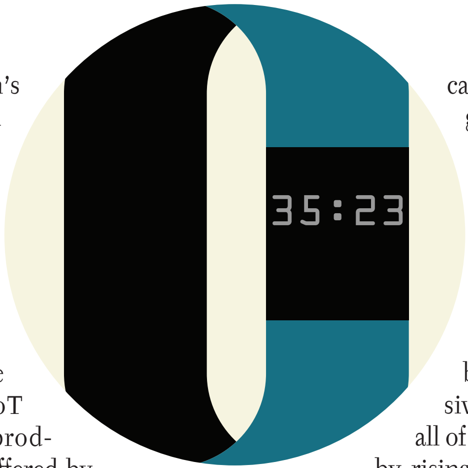


In most higher education institutions, implementing a third-party solution—hardware, software, SaaS, or hybrid—requires a supporting infrastructure for that solution. I call this supporting infrastructure a socket. The customer institution must create a socket that allows the vendor solution to interface 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

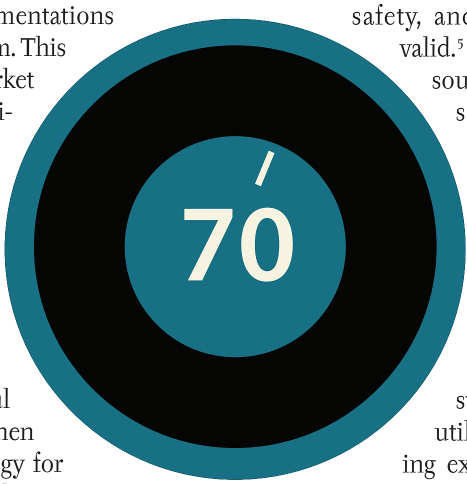
The vendor count for IoT systems being managed by an institution will only increase in the coming months and years and will likely increase substantially. Some of this increase will be from traditional systems like HVAC, which have been in the space longer than most and are maturing and extending their 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 standard frameworks that can be deployed to support requirements from multiple IoT vendors? For example, does every vendor need its own dedicated, staffed, and managed database? If vendors demand a dedicated support infrastructure, are they willing to pay for it or otherwise subsidize it?
- Are there protocols that can be leveraged across multiple vendors? Does the vendor in consideration participate in open-source protocols?
- Does the vendor offer a VM (virtual machine) image or similar approach that will work in the institutional data center or with the institutional cloud provider? Does the vendor offer a service that helps integrate its VM image into the data center or cloud environment?
- 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.[5] 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.

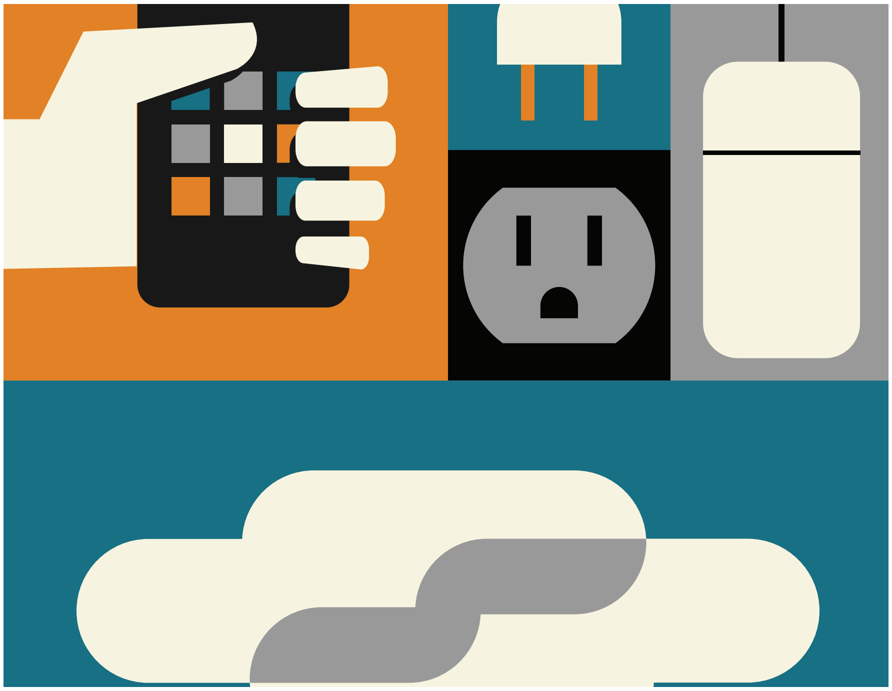
First, the IoT defies traditional classification/categorization and is still little understood. People have a hard time understanding the concept. To begin to manage IoT risk, institutional leaders must have some vocabulary for it. The IoT is still new, its effects are largely unknown and likely emergent, 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

1. Zoe Mendelson, "Chicago's Array of Things May Give Big Data Boost to Urban Planning," *Next City*, October 13, 2015.
2. Dale Evans, *The Internet of Things: How the Next Evolution of the Internet Is Changing Everything*, Cisco Internet Business Solutions Group (IBSG), white paper, April 2011, p. 30.
3. "New IDC Forecast Asserts Worldwide Internet of Things Market to Grow 19% in 2015, Led by Digital Signage," press release, May 19, 2015.
4. Dirk Chatelain, "It's a New Ball Game in Omaha, and Seems Like Seams Are a Hit So Far," *Omaha World-Herald*, June 20, 2015.
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."

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.

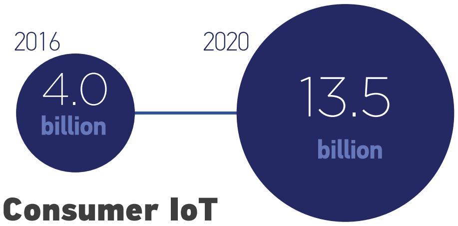
EDUCAUSE RESEARCH SNAPSHOT

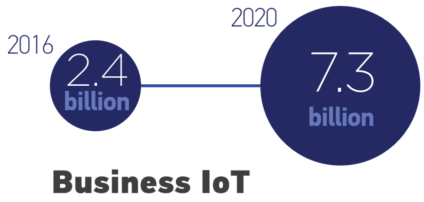
FROM BYOD TO THE IoT

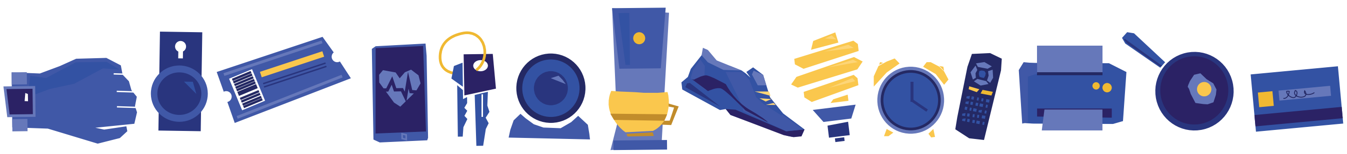
Growth of the Internet of Things

4 BILLION

consumer "things" are connected to the Internet. Gartner estimates that there will be more than three times as many connected things in 2020 as there are in 2016.[1]







"The number of items that can include a sensor is nearly limitless, and the more data are collected, the greater the need to find new ways to discover and catalog that information."

ELI 7 Things You Should Know About the Internet of Things[2]

Campus network readiness

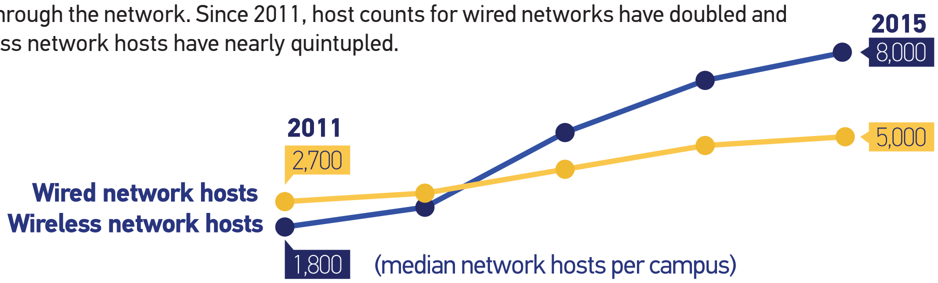
To support the IoT on college/university campuses, wireless network infrastructure needs to be secure, ubiquitous, and scalable. Higher ed is moving toward the 802.11ac standard.

	2011	2012	2013	2014	2015
802.11a/b/g	166	96	50	31	0
802.11n		100	182	264	280
802.11ac				0	50

(median number of access points for main campus)

Is higher ed ready to tackle proximal connectivity over Wi-Fi or self-optimized networks?

The size and scope of campus data networks will need to grow as more, new, and varied data flow through the network. Since 2011, host counts for wired networks have doubled and wireless network hosts have nearly quintupled.



"The increasingly connected network of devices and data streams could coordinate campus physical spaces, integrating information from sensors embedded in objects including library resources, whiteboard writing surfaces, gameboards, and robots."

ELI 7 Things You Should Know About the Internet of Things[2]

Considerations and implications for the Internet of Things (IoT) in higher education

"The Internet of Things is expected to be mainstream in universities and colleges within four to five years."

NMC Horizon Report: 2015 Higher Education Edition[3]

The complex ecosystem of the IoT

Results from the 2015 EDUCAUSE Top 10 IT Issues survey suggest that through 2021, higher ed will be growing capacity for next-gen Wi-Fi and IPv6 and will be experimenting with uses of the IoT.

Access for all kinds of endpoints and objects, including RFID- and GPS- based devices, is important at 12% **of institutions**

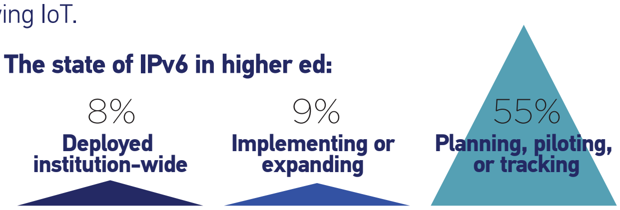
Estimated 5-year adoption trends

	2016	2019-2021
IoT	experimental	experimental
IPv6	experimental	growing

Connections and endpoints

All Internet-connected devices need an IP address. IPv4 can accommodate only about 4.3 billion connections so IPv6 is critical for anticipating connections from the growing IoT.

The state of IPv6 in higher ed:



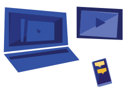
Endpoints and gateways

IoT endpoints can connect to an intermediary device or system. For consumers, this is typically a smartphone, tablet, or laptop, and for businesses, this can be a network or database. In this way, the appetite for IoT-related IP addresses will be mitigated somewhat by students' gateway BYOD devices and locally hosted systems.

The majority of students try to connect at least two devices to the campus network at the same time.

Just one
32%

At least two
61%

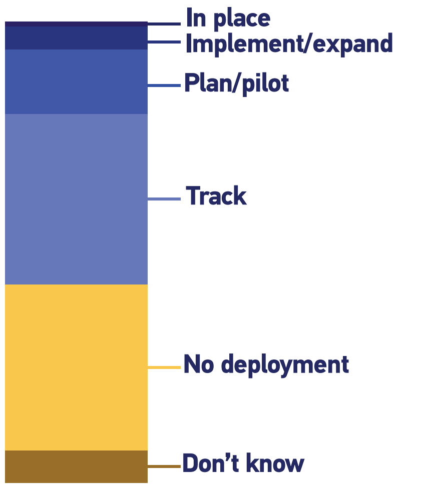


Three or more
11%

Data and analytics tools and talent

While the IoT is having a limited impact on higher ed today, the future influence could be significant, given the projected proliferation of consumer-level IoT technologies. In 2015, 37% of institutions were devoting attention to the technologies used to track uses of the Internet of Things.

Technologies that use the IoT are deployed in fewer than 10% of institutions



IoT data are new and varied (e.g., machine data from sensors, image data from cameras, behavioral data from "smart" student ID cards) when compared with data from standard enterprise information systems. Higher ed must invest in the tools and talent needed to capture, store, integrate, analyze, and use these data.

Top 3 talents needed to better use IoT data for analytics:

92% predictive modeling
89% analytics tool trainings
88% data visualization

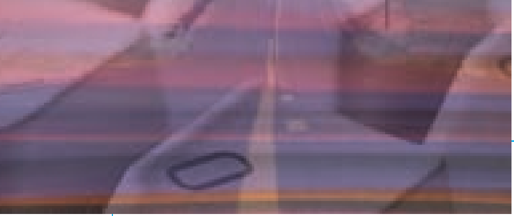
(percentage of institutions saying more positions are needed)

For more information and resources about the Internet of Things in higher education, visit the EDUCAUSE library (http://www.educause.edu/search/gss/internetofthings).

Sources:

1. Gartner Newsroom. "Gartner Says 6.4 Billion Connected 'Things' Will Be in Use in 2016, Up 30 Percent From 2015" (http://www.gartner.com/newsroom/id/3165317), 2015.
2. EDUCAUSE Learning Initiative. "7 Things You Should Know About the Internet of Things" (https://library.educause.edu/resources/2014/10/7-things-you-should-know-about-the-internet-of-things), 2014.
3. New Media Consortium. "Horizon Report - 2015 Higher Education Edition" (http://cdn.nmc.org/media/2015-nmc-horizon-report-HE-EN.pdf), 2015.

Additional data were sourced from the EDUCAUSE Core Data Service (http://www.educause.edu/core-data) and EDUCAUSE Center for Analysis and Research (http://www.educause.edu/ecar).



Community Colleges: Somewhat Different

Collaborating. Sharing. Advising. Supporting. Asking and answering. Commiserating. EDUCAUSE is incredibly important to all of us as it provides the venues, both physical and virtual, where we can engage in these activities with each other. And the value we gain from all working together is due to the fact that we are more alike than dissimilar in the services and support that we provide to our IT organizations and higher education institutions. We gather at local and regional meetings to hear peers talk about projects they are working on because we know that there is a very high likelihood we either are working on the same type of initiative or have talked about doing so. We participate in online discussion groups because we realize than when someone posts a hot issue of the moment, there is a good chance we are experiencing the same issue, have experienced the same issue, or soon will experience the same issue.

Yet we are also somewhat different from one another. We might share similar issues, but various twists make our situations unique to each of us. For example, the #1 issue on the EDUCAUSE Top 10 IT Issues list for 2016 is *Information Security*.[1] But though some IT organizations charge their chief information security officer and staff with worrying about and planning for data security, others simply ask staff members with other duties to temporarily change hats, and roles, when a data security concern arises. Or consider the #6 issue on the top 10 list: *IT Funding Models*. Whereas some higher education institutions might plan to use endowment draws or the revenue derived from tuition increases to meet current and anticipated technology needs, others have little ability to control their overall budgets—let alone their IT budgets—since their budgets are appropriated on a yearly basis by a state legislative body. Finally, *E-Learning and Online Education*, at #10 on the list, has some institutions examining how to move more of their curriculum online, while others face the challenge of addressing the fact that some (or many) members of their student body have a lack of access to the Internet or technology when not on campus.

This column was created as a way to share some of the issues unique to community colleges but also of interest to the broader membership.

Community colleges are often in the "somewhat different" category. Our institutions frequently don't have the ability to hire more staff to meet new technology challenges; instead, we ask our existing staff to change roles as often as a NASCAR driver changes hats at the end of a race. Although community colleges have infrastructure needs similar to those at other institutions, we struggle with long-range planning and funding for technology procurement and replacement, since a large portion of our budgets are at the yearly discretion of legislatures and many of us have not seen a tuition increase in four or more years. And though all higher education institutions are engaged in conversations about the role of online education, open-access community colleges must respond to the very disparate needs of their students: from those who can readily afford technology to the often large population of students for whom owning a computer, or having access to the Internet, takes a very distant backseat to buying food, paying bills, and finding and keeping a place to live.

John O'Brien, president of EDUCAUSE, recognizes the differences between various types of higher education institutions and understands the need for EDUCAUSE to support the often unique needs of community colleges. To this end, John included a special focus group on community colleges as a part of the EDUCAUSE 2016 strategic planning initiative. And this column, Connections: Community College Insights, was created as a way to share some of the issues, ideas, and concerns that might be unique to community colleges but that also might be of interest to the broader membership and that would certainly benefit from wider input.

In February 2016, Celeste Schwartz and I became coleaders of the EDUCAUSE Community Colleges Constituent Group (CG). This CG, one of only 7 (out of 51 total) that focus on particular types of educational institutions, even has the notion of being somewhat different in its description: "Many of the problems and solutions relevant to community and two-year colleges are different from those of other types of institutions. This constituent group focuses on how to manage technology-based information resources in the community college environment."

We will be using the Community Colleges CG listserv to discuss not only the issues that are unique to our types of institutions but also more broadly applicable topics that might have a slightly different feel at our two-year, public institutions. I recently reached out to group members to ask what they felt we should be discussing in the coming months. Although many of the suggested topics mirror those included in the 2016 EDUCAUSE Top 10 IT Issues list, some might be spotted only on the technology radar of community colleges:

By BRET INGERMAN

Scott Roberts © 2016

- Supporting traditional educational needs while also filling some of the highly specialized technology needs associated with degrees and certificates in fields such as nursing, firefighting, dental hygiene, and police training
- Recognizing the emerging role of open educational resources (OER), which not only can reduce educational costs to community college students, many of whom have significant financial challenges, but also hold the promise of ensuring that all students have access to educational materials on day one, which helps ensure success
- Addressing the sometimes significant lack of technology funding, or even the decreases in already limited funding, at institutions that do not have large (or any) endowments or the ability to raise tuition
- Ensuring that we can meet and balance the technology needs of students who want to bring their devices to class with the technology needs of those students who have no access to technology at home or at all

In the coming months, the Connections: Community College Insights column will be bringing forward more of the topics that are of particular concern to community colleges and two-year institutions. If you are interested in being a part of the discussion, we welcome you to join the Community College CG—regardless of your current position or type of institution. Because even though we all may be "somewhat different" from one another, we are more alike than dissimilar, and we all benefit from sharing, collaborating, and commiserating. ■

Note

1. Susan Grajek and the 2016 EDUCAUSE IT Issues Panel, "Top 10 IT Issues, 2016: Divest, Reinvest, and Differentiate," *EDUCAUSE Review* 51, no. 1 (January/February 2016).

Bret Ingerman (ingermab@tcc.fl.edu) is vice president for information technology at Tallahassee Community College (TCC) in Tallahassee, Florida. He is coleader of the EDUCAUSE Community Colleges Constituent Group.

Campus Support Systems for Technical Researchers Navigating Big Data Ethics

Complex data sets raise challenging ethical questions about risk to individuals who are not sufficiently covered by computer science training, ethics codes, or Institutional Review Boards (IRBs). The use of publicly available, corporate, and government data sets may reveal human practices, behaviors, and interactions in unintended ways, creating the need for new kinds of ethical support. Secondary data use invokes privacy and consent concerns. A team at Data & Society recently conducted interviews and campus visits with computer science researchers and librarians at eight U.S. universities to examine the role of research librarians in assisting technical researchers as they navigate emerging issues of privacy, ethics, and equitable access to data at different phases of the research process.[1]

New Ethical Dilemmas

As noted, computer science researchers face new ethical dilemmas when they conduct big data research, especially research that uses social media data or scrapes "public" information off the web. The traditional model of seeking informed consent at the beginning of a research study is often insufficient when it comes to big data research. In addition, secondary use of human subjects data collected by a third party falls into a gray area: it is considered "exempt" and not reviewed by IRBs because the data was already collected. However, some researchers consider that a loophole and advocate for greater oversight of this frequent practice due to the threat of reidentification or privacy violations that become possible through the continued analysis or aggregation of the data.

> Research librarians have a unique role to play in figuring out how we should handle the data being collected about us and where we go from here.

The acquisition of online public data carries terms of service (TOS) requirements that raise logistical and ethical challenges such as replication, identification, and consent. Growing interest in web scraping of online data raises questions about the use of online information, rules of mass downloading of data, copyright, and legal access to data.

When making decisions about data storage, researchers must take into account current security issues as well as unknown future possibilities for data breaches and reidentification. Finding the right repository involves many factors. One university we visited offers a resource that matches project characteristics with the appropriate storage. Regardless of the storage location chosen, there is widespread and prevalent concern over whether data is truly secure. One researcher we interviewed bought his own servers to store data rather than using university servers, which can be accessed by IT staff. Once the data is anonymized and aggregated, he stores it on the university supercomputers. Beyond the most sensitive and well-protected data, ambiguity surrounds what instructions or criteria a researcher should follow in deciding when to take more protective measures. IT and other departments offer guidance, but inconsistencies and confusion remain, since advice may not always be sought, followed, or clearly conveyed.

There is a growing set of requirements for sharing raw data with journals for replicability and for sharing and disseminating federally funded research with the public for potential reuse. Fulfilling data-sharing mandates is complicated, ambiguous, and potentially risky. Sharing requirements cause concern about potential privacy issues such as reidentification. Some researchers fear that sharing will lead others to misinterpret or draw different conclusions from their data. Regarding these issues, Christine L. Borgman writes: "They [scholars] need tools, services, and assistance in archiving their own data in ways they can reuse them, which increases the likelihood that their data will be useful to others later."[2]

Formal Research Support and Mandates

The IRB is often seen as the campus legal and ethics oversight mechanism for protection of human subjects. While researchers may learn ethical principles through the restraints of the IRB and value its legal and procedural oversight, many researchers say the IRB is not the best mechanism for considering potential ramifications of big data ethics overall, since human subjects protections are just one component of ethics. IRBs struggle with questions such as whether deidentified data is human subjects data, how to assess whether data can be reidentified, and how to deidentify data while still retaining its research value.[3] Secondary data use is generally considered exempt by IRBs and not part of traditional review, but changes to research methods resulting from big data have drawn this exemption into question as the distinction between primary research and secondary research has become increasingly blurry. In our interviews, IRBs were often criticized as lenient, bureaucratic, and slow, all of which can tempt researchers to cut corners.

E-Content Editor: Robert H. McDonald

By Bonnie Tijerina

Funder requirements for Data Management Plans (DMPs) were meant to encourage researchers to think through their work with data, but many see this as a hurdle. Assistance is available—such as the DMPTool (https://dmptool.org/)—and at one university we visited, representatives plan to have the library review all DMPs before proposals go to the funding agency. Many researchers we interviewed said they informally swap and copy language and see this as another item to check off a list.

Informal or inconsistent policies of publications and conferences leave researchers unsure, which affects their ability to publish or present their work. There are mixed opinions on what the role of journal review boards and conference program committees should be in determining whether submitted work is ethical and on what should be required to make their review process fair and consistent. Professional associations often lack review policies, leaving the protocol up to individual reviewers. Program committee reviewers have inconsistent approaches and often simply trust the researcher.

Informal Networks

Computer science researchers receive little to no formal or systematic ethics training during their education, compared with researchers in medicine or psychology. The former often use informal networks or conversations to make ethical decisions in their work, or they learn from their advisors in an apprenticeship relationship as they encounter issues for the first time. Requirements such as IRB training or Responsible Conduct of Research (RCR) provide some basics. However, researchers generally learn ethics on the job, through good and bad experiences, and from ad hoc conversations with other graduate students or peers.

Various formal and informal structures and services help to fill this gap on campus. Yet knowledge of these mechanisms is often shared simply through word of mouth; they are not always universally used and sometimes are made visible only following a violation.

Libraries' Unique Position

Many research libraries have increased their Research Data Management (RDM) services in recent years. From what we saw in our project, libraries have several straightforward ways to increase their support for researchers. The legal use of information is sometimes complex to navigate, but libraries have been providing copyright, IP, and Creative Commons resources on campuses for a while. There may be a role for libraries to help researchers navigate murkier areas such as data ownership, TOS violations/advice, and web scraping concerns.

Libraries have increased their support of larger and more diverse files in their repositories over time. As needs for safe, secure, and long-lasting research repositories increase, more libraries will host robust data repositories or will partner on campus or with a consortium of organizations to create data repositories, especially for potentially sensitive data. As catalogers of knowledge, libraries need to be creating and thinking through metadata to safeguard the security and privacy of sensitive data sets. This metadata can help ensure that any sensitive data is wrapped with the proper descriptive information for future sharing.

When libraries advocate for open access, open science, and open data, they must take the next step and help support the means for making data open and sharable—they must have the difficult conversations about ensuring privacy and confidentiality and protecting against potential unintended future uses of data. As a profession concerned about privacy, intellectual freedom, and the public good, librarians have a unique role to play as we all figure out how we should handle data being collected about us, how we think about future uses of it, and where we go from here.

Training and Partnering

Across our interviews, we heard concern about these emerging ethical issues. Some institutions have started lecture series or are including a segment on data ethics in their classes. The Council for Big Data, Ethics and Society, a Data & Society initiative funded by the National Science Foundation, recommends embedded training within computer science classes as early as possible, integrating ethics training with the course materials and course projects rather than as a separate module, training, or course.[4] At one campus we visited, a data clinic grew out of the statistics consulting clinic. Could a data-focused drop-in location be a checkpoint for helping researchers with their questions about the legality, privacy, or reproducibility of their work?

We also see a need for a centralized organization or initiative that can support researchers' needs throughout the research lifecycle. This may be an opportunity for the research library, as a central hub. Librarians have a key set of values and skills. From offering training in data science to helping clarify gray areas, research librarians can benefit and support technical researchers as they navigate the emerging issues of big data ethics. ■

Notes

1. The Alfred P. Sloan Foundation funded this pilot project.
2. Christine L. Borgman, *Big Data, Little Data, No Data: Scholarship in the Networked World* (Cambridge, MA: MIT Press, 2015), 282.
3. PRIM&R (Public Responsibility in Medicine and Research), "Big Data Research: Practical Solutions to Emerging Problems for IRBs," webinar, February 10, 2016.
4. Jacob Metcalf, Kate Crawford, and Emily F. Keller, "Pedagogical Approaches to Data Ethics," Council for Big Data, Ethics, and Society report, April 21, 2015.

Bonnie Tijerina (bonnie@datasociety.net) is researcher and former fellow at Data & Society (http://www.datasociety.net) in New York City.

Winona Ryder and the Internet of Things

"In the living room the voice-clock sang, Tick-tock, seven o'clock, time to get up, time to get up, seven o'clock!"

—Ray Bradbury, "There Will Come Soft Rains"

The 2015 film *Experimenter* is based on the true story of Stanley Milgram, the Yale University psychologist who became famous for his 1961 social behavior experiments that tested the obedience of volunteers who thought they were administering electrical shocks to strangers. In the film, the character of his wife, Alexandra "Sasha" Milgram, is played by Winona Ryder, and she serves as the on-screen stand-in for the film audience. Our ethical response to what happens in the film is registered on her face. In several scenes, the camera focuses on the face of Winona Ryder watching the experiment unfold—her skin twitching, her body shifting uncomfortably, her eyes wide with both horror and also a certain awe at what humans are capable of.

In his experiment, Milgram asked a "teacher" (the subject of the experiment) to shock a "learner" (an actor) for getting wrong answers on a simple test. An "experimenter" would order the teacher to give increasingly powerful shocks, and more often than not, the teacher complied. The study is not without baggage,[1] but the results remain compelling nonetheless. At one point in the film, Winona Ryder as Sasha Milgram asks to experience the shock herself, the same very small shock that the teachers were also given during the setup of the experiment. The scene is played out with a certain menace as the various accoutrements are put into action. Visually, she is overwhelmed by the devices that surround her: the electrodes, the teacher's microphone, a series of digits that light up to show the learner's answers, a pen, a clipboard, the gray of the experimenter's lab coat, a recording device, and the large box of switches through which the teacher delivers the shocks.[2] All of the devices play clear roles in maintaining and even eliciting compliance. And the subtler and more intricate or inscrutable the mechanism, the more compliance it appears to generate—because the human brain fails to bend adequately around it. The camera works a similar magic on the film viewers as it ominously traces over these objects. Like our on-screen surrogate, Winona Ryder, we too sit still—complicit, both horrified and awed by what we see and our inability to stop it.

The more we imagine our tools as transparent or invisible, the less able we are to take ownership of them.

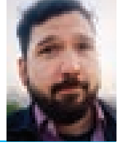
In the 1915 book *Schools of To-Morrow*, John Dewey wrote: "Unless the mass of workers are to be blind cogs and pinions in the apparatus they employ, they must have some understanding of the physical and social facts behind and ahead of the material and appliances with which they are dealing." The less we understand our tools, the more we are beholden to them. The more we imagine our tools as transparent or invisible, the less able we are to take ownership of them.

At the interview for my current job at the University of Mary Washington, the inimitable Martha Burtis asked me to reflect on the statement: "It's teaching, not tools." What assumptions does this oft-bandied-about phrase make? What does it overlook? Like Martha, I find myself increasingly concerned by the idea that our tools are without ideologies—that tools are neutral. Of course, they aren't. Tools are made by people, and most (or even all) educational technologies have pedagogies hard-coded into them in advance. This is why it is so essential that we consider them carefully and critically—that we empty all our LEGOs onto the table and sift through them before we start building. Some tools are decidedly less innocuous than others. And some tools can never be hacked to good use.[3]

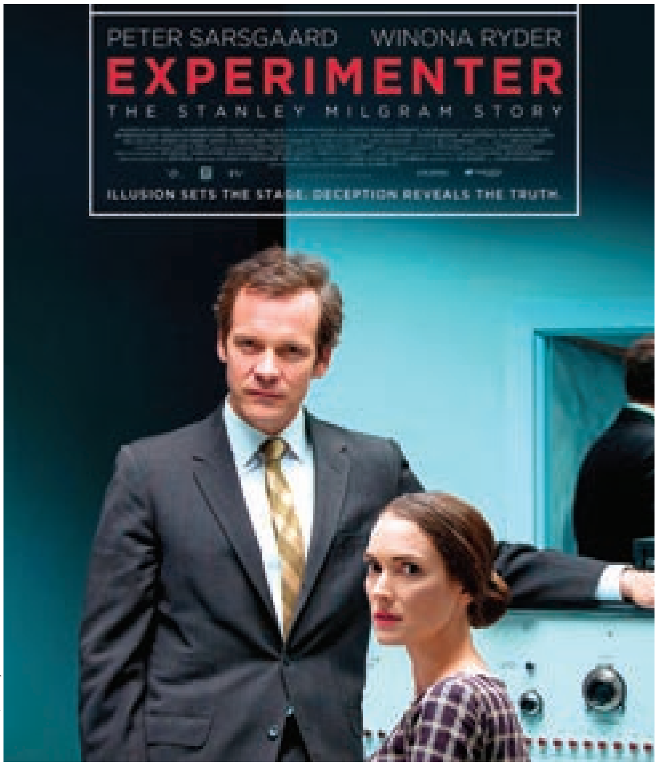
In 2014, the EDUCAUSE Learning Initiative (ELI) report "7 Things You Should Know About the Internet of Things" noted: "The Internet of Things (IoT) describes a state in which vast numbers of objects are interconnected over the Internet and can collect data and transmit and receive information. . . . The IoT has its roots in industrial production, where machine-to-machine communication enabled the manufacture of complex items, but it is now expanding in the commercial realm, where small monitoring devices allow such things as ovens, cars, garage doors, and the human heartbeat to be checked from a computing device."[4] At the point when our relationship to a device (or a connected series of devices) has become this intimate, this pervasive, the relationship cannot be called free of values, ethics, or ideology.

I'll be candid. I am quite often an unabashed fan of the Internet of Things. I like that my devices talk to one another, and I enjoy tracking my movement and my heart rate. I even find myself almost unable to resist my curiosity about something like the new Bluetooth-enabled cup that can track how much water I drink. I like controlling my car from my phone

New Horizons Editor: **Shelli B. Fowler**



BY JESSE STOMMEL



Photos 12 / Alamy © 2016

and feeling the tickle of an incoming text message on my wrist. But my own personal curiosity and fascination are outweighed by my concern at the degree to which similar devices are being used in education to monitor and police learning.

The ELI report continues: "E-texts could record how much time is spent in textbook study. All such data could be accessed by the LMS or various other applications for use in analytics for faculty and students." I am worried by how words like "record," "accessed," and "analytics" turn students and faculty into data points. I am worried that students' own laptop cameras might be used to monitor them while they take tests. I am worried that those cameras will report data about eye movement back to an algorithm that changes the difficulty of questions. I am worried because these things take us further away from what education is actually for. I am worried because these things make education increasingly about obedience, not learning.

Remote proctoring tools can't ensure that students will not cheat. The LMS can't ensure that students will learn. Both will, however, ensure that students feel more thoroughly policed. Both will ensure that students (and teachers) are more compliant. In his 1974 book *Obedience to Authority: An Experimental View*, Milgram described "the tendency of the individual to become so absorbed in the narrow technical aspects of the task that he loses sight of its broader consequences." Even if I find the experiment itself incredibly problematic, Milgram offers useful reflections on the bizarre techno-theater that helped elicit obedience.

When Internet-enabled devices have thoroughly saturated our educational institutions, they run the risk of being able to police students' behavior without any direct input or mediation from teachers. By merely being in the room, the devices will monitor students' behavior in the same way that the cameras and switches and lab coats did in Milgram's experiments. How will learning be changed when everything is tracked? How has learning already been changed by the tracking we already do? When our LMSs report how many minutes students have spent accessing a course, what do we do with that information? What will we do with the information when we also know the heart rate of students as they're accessing (or not accessing) a course?

I maintain a great deal of excitement about the potential of the Internet of Things. At the same time, I find myself pausing to consider what Milgram called "counteranthropomorphism"—the tendency we have to remove the humanity of people we can't see. These may be people on the other side of a wall, as in Milgram's experiment, or people mediated by technology in a virtual classroom.

Winona Ryder has very few lines of dialogue in *Experimenter*, and yet her performance is a pivotal one because she offers a guide, a moral compass, for the off-screen audience. She is complicit in her passivity and yet rebellious in her willingness to register raw and genuine emotion, something no other character can muster. And as the film unfolds, the shock and awe on her face gives way to compassion. As she looks upon the scene of the experiment, she sees human beings and not the experiment.

We must approach the Internet of Things from a place that doesn't reduce ourselves, or reduce students, to mere algorithms. We must approach the Internet of Things as a space of learning, not as a way to monitor and regulate. Our best tools in this are ones that encourage compassion more than obedience. The Internet is made of people, not things. ■

Notes

1. Cari Romm, "Rethinking One of Psychology's Most Infamous Experiments," *The Atlantic*, January 28, 2015.
2. Milgram described this last device as "an impressive shock generator. Its main feature is a horizontal line of thirty switches, ranging from 15 volts to 450 volts, in 15-volt increments. There are also verbal designations which range from SLIGHT SHOCK to DANGER—SEVERE SHOCK." (Stanley Milgram, *Obedience to Authority: An Experimental View*, 1974) I sense glee in the language Milgram uses ("impressive"), something theatrical in his excess ("thirty switches"), and a fastidiousness in his attention to detail in reporting all of this.
3. Jesse Stommel, "Who Controls Your Dissertation?" *Vitae*, January 7, 2015.
4. EDUCAUSE Learning Initiative (ELI), "7 Things You Should Know About the Internet of Things," October 6, 2014. I find something ominous about the capital I and capital T in the acronym IoT, a kind of officiousness in the way these devices are described as proliferating across our social and physical landscapes.

Jesse Stommel (Twitter: @Jessifer) is executive director, Division of Teaching and Learning Technologies, at the University of Mary Washington. He is the director and founder of Hybrid Pedagogy (http://www.hybridpedagogy.com) and Digital Pedagogy Lab (http://www.digitalpedagogylab.com/). His own personal site is at http://www.jessestommel.com.

The Internet of Things Is Here

The Internet of Things (IoT) is a topic that engenders excitement, skepticism, and anxiety. Supporting these feelings are expectations regarding the potential value that the IoT can create today and into the future, the "hype-cycle" considerations, and the risks regarding security and privacy. Yet the fact is, the Internet of Things is here. Now. Higher education thus has an opportunity to support the development and deployment of the technical and business model innovations for an IoT-enabled economy, to build the leaders of the IoT-enabled economy today and into the future, and to address the TIPPSS risks related to the IoT: **T**rust, **I**dentity, **P**rivacy, **P**rotection, **S**afety, and **S**ecurity.

The current reality of the IoT is already staggering, not even considering the expectations and hype about the future: billions of physical devices, across the world, that have digital sensors and are interconnected by leveraging the Internet or other network technology. An estimated 13.4 billion devices were connected in 2015, representing more than twice the human population on the planet at the time, and this number is projected to nearly triple, to 38.5 billion devices, by 2020.[1]

Connecting the physical to the digital world can encompass a wide range of objects: vehicles, appliances, lighting, health and wellness devices, manufacturing systems, buildings, bridges, water pipes, food containers, electric meters, security systems, cameras, wearable devices, drones, and many more. These objects are connected through a digital sensor that collects and transmits data to other devices or to a centralized management system. The public Internet or private networks connecting these devices provide the communications between these devices—or "things."

A report recently published by Internet2 highlights the IoT at the top of the "Key Information and Communications Technology Trends for the Research and Education Community" through 2025.[2] According to some estimates, the IoT could create $11.1 trillion in global economic value by 2025, representing 11 percent of global gross domestic product (GDP).[3] This economic value reflects both the upside revenue potential for IoT-related devices, applications, and services and also the efficiencies and cost reductions generated through the IoT. This multi-trillion-dollar opportunity not only attracts investments but also requires innovation in technology and business models to be enabled. The risk factors of the IoT require additional research and development.

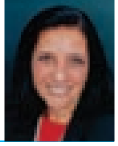
The higher education community can lead the development of the technologies, business models, ethics, and leaders of the IoT-enabled world. For example, professors of engineering and computer science are directing IoT labs for the improvement of IoT technologies, including security design. They can work with business schools to design curricula and form IoT clubs to create new business models. Law schools can teach IoT ethics, privacy, and policy. Medical schools can enable the "Internet of Medical Things." Informatics programs can teach how to leverage the volumes of IoT data, with TIPPSS. Through such efforts, the higher education community can work across disciplines to develop the technologies, business models, and leaders for the IoT-enabled economy of the future.

The Importance of the IoT to Higher Education

1. *The IoT is on campus now.* Whether we're ready or not, the IoT has already infiltrated the university experience. Students are coming to college with an average of seven unique IoT devices.[4] Since students are arriving on campus with so many devices, higher education institutions can leverage this opportunity to enhance the student experience on several fronts. For instance, they can use students' smartphones and smartwatches as a communications mechanism. At Virginia Tech, the VT Alerts (https://www.alerts.vt.edu/) system notifies students, staff, and faculty of a campus emergency situation. Starting at the University of Washington, a student-developed app—OneBusAway (http://onebusaway.org/)—provides real-time information for metro-area bus systems not only in Puget Sound but also in other cities across the country. Leveraging the IoT, smart campuses can be test beds for early IoT innovations to inform decision making for the surrounding cities and communities and can serve in public-private partnerships.

2. *The IoT needs discovery and development—which researchers, educators, and students in higher education can lead.* Higher education researchers, educators, and students are in a unique place to lead the discovery and development of IoT devices, applications, systems, and services. At the 2016 South by Southwest (SXSW) interactive festival, U.S. President Barack Obama said he was there to recruit attendees to develop new platforms and ideas across disciplines and across skill sets to solve some of the big problems we're facing today.[5] IoT and analytics technology can be leveraged to capture and analyze data and provide actionable insights to improve health and wellness with the connected "Internet of Medical Things," to improve efficiencies on campus and across communities, to reduce energy use, and to improve information capture to address public safety issues. This will require working across skill sets and disciplines to build a system view. Researchers can create end-to-end TIPPSS solutions for the IoT, including for life-critical applications such as connected health devices and connected vehicles. Researchers, educators,

Viewpoints Editor: **John Suess**



Getty Images, Yagi Studio © 2016

and students can build IoT devices and services with a "defense in depth" strategy, adding in security at the hardware, firmware, software, and service levels.

3. *Higher education needs to build the leaders of the future IoT economy.* The sophisticated talent within higher education systems will envision, develop, and lead the new business model and technology innovations. The future of the IoT economy can be shaped by experts and leaders in higher education and by the students they are educating. For example, the University of Wisconsin–Madison Internet of Things Lab (http://www.iotlab.wisc.edu/) is shaping technical innovation skills as students are learning to create IoT apps and end-to-end systems from devices speaking with other local devices such as in a smart home, communicating over a network to centralized management systems (e.g., building management systems), and to applications in the cloud. The UW-Madison IoT lab has become a campus hub for multidisciplinary education, research, and university-industry collaboration to learn, explore, and innovate with IoT technologies and applications in various domains. Beyond technical innovations, leaders in higher education can also guide new business model innovations, using IoT-enabled systems to create new services, improve client service, and integrate and analyze data from disparate but related systems to increase efficiencies and add value to businesses and consumers. Higher education has the opportunity to shape the future leaders of an IoT-enabled economy by designing curricula for technical and business leaders and by facilitating students and researchers to build new business processes that leverage IoT technologies in a multidisciplinary way.

Join the IoT Journey

In February 2016 the IEEE, the National Science Foundation (NSF), and Internet2 cosponsored a workshop, "End to End Trust and Security for the Internet of Things," followed by an IEEE Experts in Technology and Policy Forum at George Washington University in Washington, D.C.[6] These workshops attracted IT, research, academic, industry, government, lab, agency, and networking leaders, resulting in a series of technical considerations and a discussion on IoT policy and ethics. The ease of developing an IoT application can lead to risks of device and individual TIPPSS. As noted above, law and business professors are beginning to consider how we might design a point of view and curriculum regarding IoT ethics.

To enable higher education leadership, discovery, and development for the IoT, Internet2 offers several initiatives that campuses can join, including the IoT working group and the end-to-end trust and security working group. The IoT working group convenes higher education, industry, and government agency leaders to advance technology and ongoing innovation, ushering in a new era of the IoT. Internet2 has also launched a Smart Campus Initiative—led by a higher education CIO advisory council—to identify, develop, and enable the scaling and securing of IoT solutions across colleges and universities. Higher education leaders will be working together to create and share experiences regarding new IoT-enabled systems that improve efficiencies, energy use, the student experience, and the athletic fan experience and that integrate systems across a campus and community for a better quality of life. As part of the smart campus and IoT initiatives, Internet2 also established a task force on IoT systems risk management to identify the IoT-related risks and suggest recommendations for risk mitigation.[7]

Higher education has the resources and talent to develop and shape the future of the IoT, especially since it is already on our campuses. This is a topic that should be top-of-mind for college and university presidents, CIOs, researchers, educators, and technical staff as they build and position their institutions for future success. ■

Notes

1. Juniper Research, "'Internet of Things' Connected Devices to Almost Triple to over 38 Billion Units by 2020," press release, July 28, 2015.
2. Florence D. Hudson, "Key Information and Communications Technology Trends for the Research and Education Community," Internet2, February 2016.
3. James Manyika, Michael Chui, Peter Bisson, Jonathan Woetzel, Richard Dobbs, Jacques Bughin, and Dan Aharon, "Unlocking the Potential of the Internet of Things," McKinsey Global Institute, June 2015. The World Bank projects $100 trillion per year in global GDP in 2025: World Bank World Development Indicators, International Financial Statistics of the IMF, IHS Global Insight, and Oxford Economic Forecasting, "Projected Real Gross Domestic Product (GDP) and Growth Rates of GDP for Baseline Countries/Regions (in billions of 2010 dollars), 2010–2030."
4. "College Students Own an Average of 7 Tech Devices," *MarketingCharts*, June 18, 2013.
5. "President Barack Obama Keynote Conversation," SXSW Interactive 2016.
6. "IEEE End to End Trust and Security Workshop for the Internet of Things," Washington, D.C., February 4, 2016; "IEEE Experts in Technology and Policy (ETAP) Forum on Internet Governance, Cybersecurity and Privacy," Washington, D.C., February 5, 2016.
7. For more information on these initiatives, see Internet2: "Collaborative Innovation Community"; and "April CINO Update," April 13, 2016. If you are interested in joining the Internet2 initiatives, e-mail CINO@Internet2.edu.

Florence Hudson (fhudson@internet2.edu) is senior vice president and chief innovation officer for Internet2.

Strengthening Higher Education Together

Our corporate members play a critical role in helping higher education deliver on its mission. EDUCAUSE thanks our 2016 Corporate Partners for their continued support!

PLATINUM PARTNERS

Dell, ellucian, Gartner, Jenzabar, mediasite by sonicfoundry, VeriSign, workday (Built for the future.)

GOLD PARTNERS

amazon web services, brightspace by D2L, Campus Management, CDW-G People Who Get IT, Cisco, Citrix, Epson Exceed Your Vision, Google for Education, IBM, Kaltura, McGraw Hill Education, Microsoft, Moran Technology Consulting, Oracle Education and Research, Pearson, Steelcase Education, Unit4 (In business for people.)

SILVER PARTNERS

CCI, Extron, Laserfiche Run Smarter, Lenovo, Lynda.com A LinkedIn Company, OnBase by Hyland

BRONZE PARTNERS

Blackboard, canvas, Cengage Learning, echo360 active learning, Extreme (Connect Beyond the Network), Fischer International, GovConnection (A PC Connection Company, we solve IT), Hobsons, Learning Objects, Modo Labs, NEC, Panasonic, Spectrum Industries Inc., visix, vmware

We also thank over 280 additional corporations that support our mission.

To learn more about these partners, visit **educause.edu/Corporate-Partners**.

EDUCAUSE

UNCOMMON THINKING FOR THE COMMON GOOD

Corporate Resource Guide

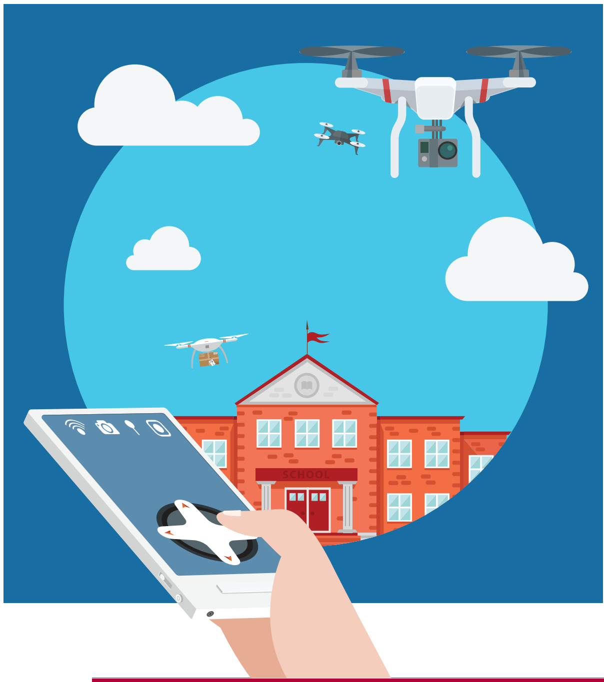
Advertiser Index

Company	Contact	Website	Page
Advantiv Corporation	1-866-966-2911	www.advantiv.com	55
Amazon Web Services – An EDUCAUSE Gold Partner		www.aws.amazon.com/education	7
AT&T	1-877-542-8666	www.att.com/security	31
Computer Comforts – An EDUCAUSE Silver Partner	1-281-535-2288	www.computercomforts.com	5
Jenzabar – An EDUCAUSE Platinum Partner	1-800-593-0028	www.jenzabar.com	inside front cover
Laserfiche – An EDUCAUSE Silver Partner	1-800-985-8533	www.laserfiche.com/leader	inside back cover
OneWorldSIS	1-434-296-8800	www.oneworldsis.com	18
Samsung	1-866-SAM-4BIZ	www.samsung.com/wlan	24–25
Spectrum Industries	1-800-235-1262	www.spectrumfurniture.com	13
Unicon	1-480-558-2400	www.unicon.net	55
UNIT4 – An EDUCAUSE Gold Partner	1-888-247-3776	www.unit4.com/us	3
Verisign – An EDUCAUSE Platinum Partner	1-703-948-3200	www.verisign.com	17
Workday – An EDUCAUSE Platinum Partner	1-925-951-9000	www.workday.com	back cover

Why IT Matters to Higher Education

EDUCAUSE review

Online in July/August »



Drones on Campus

What roles can and should drones play in higher education? Learn the benefits, risks, and recommended governance for drone use on campus.

educause.edu/ERO

Search

Systems Risk Planning and Management for the Internet of Things

Along with its benefits the Internet of Things brings a whole range of risks, from network capacity to security threats. Higher education IT departments must prepare policies and responses before the onslaught overwhelms their campuses.

Video: 7 Ways to Lead Operational Change from Where You're Standing

We don't have the luxury of addressing innovation while standing still. Here are seven ways to effect change as we move through the day-to-day operations of our IT departments.

Mobile Beacon App at the University of Oklahoma

As part of its focus on innovation, the University of Oklahoma Library uses a mobile beacon app to help students find their way through its resources and spaces.

Research into the Internet of Things

Different higher education institutions have launched research initiatives into the benefits and challenges the Internet of Things brings to society, from increased demands for rapid interconnection to privacy and security threats. Learn about a few of these projects here.

Upcoming issues will focus on analytics and a review of topics of interest to readers.
Share your work and ideas with *EDUCAUSE Review*—contact **editors@educause.edu**.

EDUCAUSE