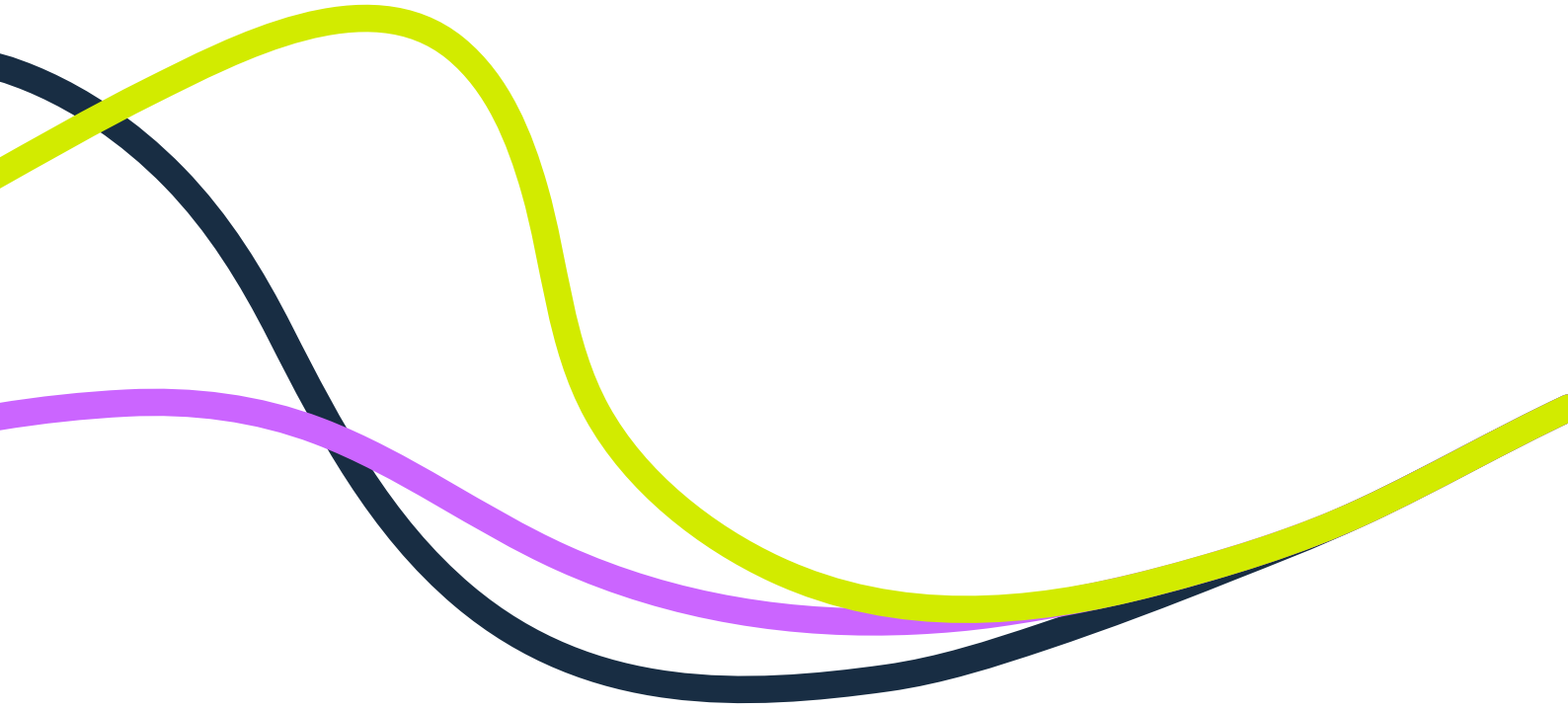
The Hoffman Agency

Smart campuses, smarter decisions: Unlocking the potential of IoT in schools

Challenges, applications, and a roadmap for adoption

Sponsored by AXIS COMMUNICATIONS

Contents



Introduction

Schools and universities have always strived to be at the vanguard of developing and using new technologies, with a particular focus on learning and research.

But despite being at the forefront of technology and research, some applications are left behind as others are prioritized. The security and safety of staff, students, and visitors is understandably top of mind when implementing IoT solutions such as access control and camera surveillance.

Meanwhile, businesses in other sectors are motivated to use technology in other ways, either to cut costs or increase revenue.

The education sector does have its priorities right, but institutions may be missing out on benefits that would improve campus operations. Addressing this is vital for a sector where budgets can be tight.

In this report, we have taken a closer look at the use of IoT in the education sector, where opportunities for actionable insights, analytics, and campus operations may be missed. We have used real-life case studies, research, and interviews with education technology experts to lift the lid on the barriers and opportunities that lie within the sector.

Executive summary

Businesses, driven by profits, often do all they can to improve efficiency and margins. But what about those organizations with a higher calling to education and research? Often, it's not that they don't have the technology, but more that they aren't using it to its full potential.

We don't see this as a failing. Educational institutions are rightly focused on their primary purpose – to educate students. And IoT technologies are used mostly to keep those in education safe.

IoT technologies and the data they capture can do much more. They can reduce costs through space optimization and energy efficiency. They can help with crowd control and anti-social behavior. They can even help make better decisions for those areas that are profit-making.

Of the barriers that stand between educational institutions and these advantages, the biggest is a lack of awareness of what IoT is capable of. However, budgetary restrictions and lapses in communication between departments don't help. Cybersecurity threats are another issue – already vulnerable, institutions can be wary of deploying more software and hardware than they need.

Educational institutions may lack the profit motive of many businesses, but that doesn't mean they shouldn't take full advantage of the efficiencies available to them.

IoT maturity: going beyond adoption

The Internet of Things: The network of physical objects embedded with sensors and software, connecting and exchanging data with other devices. These range from smart home devices to security systems to smart robotics.

IoT is already part of most, if not all, educational establishments in the developed world. In fact, many were early adopters of connected technologies. The first IoT device was a soda vending machine at Carnegie Mellon University, hooked up to sensors in 1982 by a graduate student unwilling to trek across campus, only to find it out of stock.

However, this adoption has not been uniform across the globe. Some markets are still in early or growth stages. For example, IoT adoption in Latin America is not as mature as in North America or Australia. This isn't necessarily due to an unwillingness to adopt, but due to legacy technology.

> "The biggest obstacles can be infrastructure deficit and connectivity gaps. We typically face the prevalence of legacy networks with low throughput that collapse under the demands of high-resolution video streams and metadata processing."
>
> **Ricardo Moreno,**
> *Axis Regional Sales Manager, Mexico*

Connected technology in education today tends to focus on accessibility, interactivity, and collaboration, with applications such as remote learning, interactive lessons, and peer-to-peer learning between students. Beyond this, IoT solutions tend to focus on security: access technologies, surveillance, and anomaly detection, all designed to make sure those on campus are supposed to be there, and minimizing security threats. The investment here can be significant. In 2021, it was estimated that US schools and colleges spent $3.1 billion on surveillance and security technology.

> "Campus safety is always a consideration. The goal of the security department is to make their campus as safe as possible for staff, students and visitors. What is most overlooked is energy optimization and reducing total cost of ownership. Post-secondary schools use so many devices, so finding ways to reduce power is something that can be beneficial."
>
> **Andrew Kertesz,**
> *Axis Business Development Manager, Canada*

This focus on security, while understandable, does mean gaps can exist where IoT is not fulfilling its potential.

IoT can improve campus operations, make considerable savings, and inform future planning. Fortunately, this doesn't always necessitate new or better technology, but a change in mindset around solution implementation and better knowledge of what is possible.

Barriers to adoption

To understand why the education sector has not taken full advantage of IoT, we should look closely at the barriers that prevent it.

Knowledge

You cannot implement something if you don't know it exists. Those who make decisions about implementation understand the issues at hand, but don't hold full knowledge of the solutions available that could help.

> "There is a gap between the manufacturers developing the solutions and the end customer. They just aren't aware of the different things these IoT devices are capable of."
>
> **Andrew Kertesz,**
> *Axis Business Development Manager, Canada*

This isn't necessarily a lack of knowledge of IoT systems – many will be already using, for example, surveillance systems and security cameras. But they may not know that the data from these systems can also be used to, for example, inform decisions around the use of space, crowd control measures, environmental controls, and more.

Consultants and specification

Educational institutions are tax- and donor-funded entities, and with that comes restrictions on how money is spent. One of these is how bids are tendered. Their needs are often scoped and specified by consultants. The capabilities of IoT can be lost in this process. Consultants need to not only understand the technology but also be comfortable with specifying IoT tenders.

Fragmentation of departments

Different stakeholders within an organization have different needs, and getting everyone on the same page can be difficult. For example, using surveillance technology to improve building use would mean IT, finance, security, and facilities management teams would need to be on board.

Budget

Investing in IoT solutions costs money, even if it saves money in the long term. Education budgets are often already stretched, which can mean implementing the basics and ignoring more advanced implementations. Proving return on investment is a must.

Technical debt and integration

As early adopters of some technologies, and late adopters of others, educational institutions can find themselves in a tricky position. Existing solutions may work well but lack the ability to integrate with new technologies, either because that wasn't part of planning, or because existing technologies do not use industry-wide standards.

> "Modern learning tools are only as strong as the infrastructure behind them. Aging networks and fragmented systems limit performance, slow adoption, and make scaling far more difficult. Seamless integration and true interoperability are essential to unlock the full value of connected technologies in schools."
>
> **Yung Huynh,**
> *Axis Key Account Manager, Oceania*

Cybersecurity risks

Adding more connected technology creates a greater "attack surface" for hackers, offering more routes into a network. IT specialists can mitigate the risk with regular patching and techniques such as network segmentation, but this increases ongoing cost and could increase cybersecurity risks at a time when threats are on the rise. According to one study, over half of US educational institutions have suffered a data breach in the last five years.

These hurdles are not inconsiderable, but many of them also apply to any technology purchase. The key to overcoming these objections and making full use of IoT implementations is to better understand the use cases.

IoT use cases

Many educational institutions already understand connected technology's benefits for education, and the need for IoT in security. Here, we outline some of the most common use cases for IoT beyond these, based on our conversations with local experts and technology buyers.

Improved energy use

This is a major use case. Schools and university campuses can be huge, multi-building complexes that cost a great deal of money to heat and light. A better understanding of what parts of the building are in use, peak hours, and occupancy rates can be translated into solid intelligence that informs decisions around factors such as heating and ventilation.

This has many benefits. There is saving money on energy bills, of course, but also meeting sustainability goals and providing a healthy environment for teaching and learning.

The ministry of education in Quebec has deployed over 47,000 environmental sensors province-wide to continuously monitor CO_2 and other environmental parameters. This provides real-time data to inform ventilation strategies, improving both comfort and long-term building efficiency. Ontario has followed suit and is currently supporting a grant program for educational institutions to deploy environmental sensors.

Ministry of Education, Quebec

Space optimization

Campuses are complicated systems with students, teachers, and visitors constantly moving around to attend classes, lectures and facilities. Using space efficiently can be difficult, and analysis of IoT data can uncover rooms that are underused or too crowded to help create better learning environments.

In 2024 UCLA used IoT sensors in its Space Optimization Program for summer classes. With around 75% of summer courses offered online, it was an opportunity to consolidate in-person activity into a smaller number of buildings. The program is expected to deliver insights into space utilization and occupancy patterns across facilities, reducing energy consumption and operational costs through automated environmental controls. (UCLA)

The Digital Twin of University of Queensland's St Lucia campus integrates historical, real-time, and predictive data to inform models such as flood simulations, mobility around campus and how it's affected by construction, building occupancy assessment with spatial data, and mapping of building age in relation to campus infrastructure. Benefits include improved infrastructure management through predictive analytics, greater efficiency in spatial planning and asset optimization, and enhanced research capabilities in digital humanities, engineering, and design

University of Queensland, Australia

Improved security outcomes

Access control and surveillance technologies collect data, and this data can be used to identify patterns that can help reduce security risks. However, this requires data sharing through standards and ensuring that these technologies are not "siloed".

> This approach can also help with safety beyond security, recognizing issues that go beyond unexpected visitors.
>
> As well as after-hours person detection on specific cameras, we receive alerts when cars exit our carparks the wrong way and unsafely. We can then have a conversation with them to ensure it doesn't happen again"
>
> **Nick Moseley,**
> *Head of IT, Australian private school*

Anti-social behavior

Security is not just about unwanted visitors, of course. Schools and universities want to limit anti-social behavior and create a safer learning environment. Camera surveillance helps but will always have blind spots. The combination of data and additional sensors can make a difference here – one example is the use of vape detection in areas where cameras are unsuitable.

Data-driven decisions for profit

Universities, in particular, have profit-making enterprises as part of the campus, such as on-site stores, cafes, merchandise, and more. Just as high street retailers take advantage of IoT to better understand their customers and inform decisions to increase sales, on-campus stores can do the same.

Better management of events

College sports, particularly in the US, attracts crowds that can be difficult to manage on game days. Even for smaller events, it's crucial to be equipped to manage more visitors than the campus is used to. Data can help detect patterns and issues, such as traffic congestion, queue management, overcrowding, and more.

> "Ohio State University uses AI and camera technology to manage crowds at its football games. But it's going a step further to create a better experience for attendees. By checking an app, visitors will be able to see which concession stands are less crowded, cutting down on queues and making sure no one misses the action."
>
> **EdTech Magazine**

Improved public communications

Schools and universities need to make campus-wide announcements, but with older public address systems, there's no guarantee that the message would be heard. Integration of speakers and sensors can guarantee full coverage of a campus – vital for important messages – and send alerts during ongoing incidents.

Budget

Investing in IoT solutions costs money, even if it saves money in the long term. Education budgets are often already stretched, which can mean implementing the basics and ignoring more advanced implementations. Proving return on investment is a must.

Technical debt and integration

As early adopters of some technologies, and late adopters of others, educational institutions can find themselves in a tricky position. Existing solutions may work well but lack the ability to integrate with new technologies, either because that wasn't part of planning, or because existing technologies do not use industry-wide standards.

Cybersecurity risks

Adding more connected technology creates a greater "attack surface" for hackers, offering more routes into a network. IT specialists can mitigate the risk with regular patching and techniques such as network segmentation, but this increases ongoing cost and could increase cybersecurity risks at a time when threats are on the rise. According to one study, over half of US educational institutions have suffered a data breach in the last five years.

These hurdles are not inconsiderable, but many of them also apply to any technology purchase. The key to overcoming these objections and making full use of IoT implementations is to better understand the use cases.

Factors to consider when implementing IoT solutions:

Understanding the use cases for IoT and the barriers to adoption is still only part of the solution. Every campus is unique and will have its own needs, level of current adoption, and ability to invest.

To better understand the steps that schools or universities could take, here are some of the factors that should be examined in detail:

Existing network infrastructure capabilities and solutions. Is this something that can be built upon, rather than replaced? Can current implementations share data and integrate with software platforms? Is the current network able to host the IoT solutions being proposed?

Size of the campus and population. A solution that fits an urban, multi-campus university may not be right for a small rural school. It's vital to identify specific needs alongside potential use cases, rather than make the use cases fit.

Data security and privacy. Any data collected will need to meet privacy guidelines, which can be national or state-level, and may have specific provisions for minors. Good security means ongoing maintenance, not just of the IoT devices themselves but of the entire network.

Scalability and interoperability. Planning for the future means looking at how solutions can work with what exists today, as well as future implementations. Does it use standard data formats? Can it be integrated into software platforms or does it require its own platform? Avoiding future technical debt is challenging but a must for any roll out.

Operational costs and ROI. Possibly the most important factor to consider. Any institution needs to take a realistic but forward-looking approach to IoT applications. ROI is of course important, and should be considered over the long-term, but so should the cost of maintenance and support.

IoT and new technologies

Part of planning for the long term is considering how the future may change existing technologies and where they fit in.

As use cases and benefits of IoT become clear, there will be more opportunities to integrate new technologies, elevate existing processes, and unlock new use cases.

For example, let's consider AI. Although it is here today, it is also a fast-moving, fast-changing technology. The full implications of its use, the benefits, and use cases have yet to be explored or realized.

AI thrives on data. IoT produces a lot of data. AI has the potential to create or enhance many IoT use cases. Beyond security, AI could be used for better energy use and crowd management, making predictions based on current and past data to find patterns.

> "AI can take all of the data that's gathered and turn it into information in a matter of seconds. Security systems in the past used passive recorders. With the advent of AI, we can take all of those devices and turn them into a force multiplier for all the eyes that are looking.."
>
> **Jill Renihan,**
> *Axis Segment Development Manager for Education, Americas*

Even if institutions are not ready for AI today, they need to make it part of their future. The key is remaining agile and avoid vendor lock-in or adhering to proprietary standards. By using open standards, schools and universities – and, indeed, any organization or business – will be flexible enough to integrate new technologies.

Conclusion and recommendations

Many schools and universities today have IoT solutions in place but won't be making full use of their capabilities.

The first step is to understand existing IoT implementations. For many institutions, they won't need to "rip and replace" what is already there but look to enhance what exists. Are they taking full advantage of what is in place, or could it do more? Can it be integrated with other technologies to help save money and create efficiencies?

Security will always be a priority for any school or university, but decision-makers should think beyond this need. Can their access and surveillance data be used to inform other decisions? Can it give us a better understanding of how campuses are used?

It's vital that data privacy and cybersecurity are built-in from the start. By prioritizing solutions that meet data requirements and defend against cyberattacks, schools and universities will keep valuable information safe.

Most important of all is closing the knowledge gap. By understanding what IoT is capable of, and where that fits with long-term objectives and needs, decision-makers will be in a much better position to plan. There's no need for the educational institution to do all of the heavy lifting here – consultants and vendors will help improve understanding and demonstrate ROI.

Existing IoT implementations in education, and even in other sectors such as retail or arena management, can show the possibilities, plus how ROI is achieved and measured. Every investment needs to be justified, but there are lots of case studies showing what is possible: better event management, energy and space optimization, and more.

It's also important to build for the future, using open standards where possible, collecting the right data, and using a central platform to collate data and manage the results. IoT implementation shouldn't be a one-off project, but part of an ongoing effort to improve efficiency and decision-making.

About The Hoffman Agency

Defining communications broadly to include digital, content marketing, thought leadership, as well as traditional PR, The Hoffman Agency marches to its own percussionist. One of the few independent communications consultancies with global reach, it operates offices in Europe (London, Munich and Paris), Asia (Tokyo, Seoul, Beijing, Shanghai, Taipei, Hong Kong, Singapore, Bangkok, Kuala Lumpur and Jakarta) and the U.S. (Silicon Valley, Portland and Boston). The firm supports some of the biggest brands in the world, many of which prefer to remain unnamed (the client names we have permission to share publicly are on our website).

This report conducted by The Hoffman Agency was commissioned by Axis Communications.

Sponsored by AXIS COMMUNICATIONS