

**Best Practices for
Modernizing Security Systems
in Legacy Education
Environments**





Executive Summary

Modernizing security systems in aging K-12 Schools and higher education institutions require practical strategies and proven best practices.

With the average U.S. school building nearly 50 years old and facing escalating safety risks, educational institutions must urgently update their security approaches. This paper outlines this urgent need and continues to outline how to best approach the provided best

Each best practice is designed to address real-world challenges faced by aging educational facilities and the teams that manage them. The discussion is organized into three primary categories of challenges: environmental, technical, and operational.

By identifying specific challenges and proposing best practices grounded in real-world applications, this paper equips school security teams and their stakeholders with the insights they need to enhance campus security.

Long-term success depends on maximizing the value of modernization efforts, and security consultants play a crucial role in achieving that outcome.

Contents

Understanding the Need	Page 2
Approach to Best Practices	Page 3
Addressing Legacy Challenges with Modernization Best Practices.....	Page 7
Deriving Additional Value.....	Page 16
About Atriade	Page 17



Understanding the Need

There is a strong juxtaposition between aging educational institutions and today's modern security systems.

According to the [National Center For Education Statistics](#), the average U.S. school building is 49 years old. What's more, 38% were constructed before 1970.

Conversely, modern security technologies are generally designed for environments with modern infrastructure, robust network capabilities, and flexible space planning – many things even the most prestigious educational institutions lack.

This juxtaposition exists in a world where schools and higher education campuses are facing increasing security risks.

Consider the following:

- Since 1999, [the rate of U.S. students exposed to a school shooting has nearly tripled](#), with most of the increase occurring from 2020 to 2024
- In 2022, [one out of every five students](#) reported being bullied
- E-cigarettes are the [most commonly used tobacco product among U.S. youth](#), with [9 in 10 teachers](#) saying vaping is disruptive to learning environments

Compounding these risks is the operational complexity inherent in educational settings. Not quite public but not entirely private, many are 24/7 facilities with students, faculty, and visitors on-site year-round.

Higher education campuses, in particular, often consist of multiple buildings, each potentially managed by separate departments with varying priorities and resources.

Despite these challenges, the need for modern, effective, and fully integrated security solutions has never been greater. So, how can campus security teams and their counterparts navigate the pitfalls of aging environments while still delivering the protection their stakeholders demand?



Approach to Best Practices

Before diving into detailed recommendations for security retrofits in legacy education environments, it's helpful to take a step back and consider the broader strategy.

It is not enough to simply apply a 'best practice' to a particular project and then step back and hope for the best. Modernizing security systems requires extensive planning, successful engagement with various stakeholders, and contingencies. Without these elements, even the best 'best practices' can fall short, resulting in delays, cost overruns, and increased security risks.

Developing a Plan

Every security system upgrade, retrofit, or expansion begins with a comprehensive, campus-specific plan. If you're not sure where to start, start by following the risk.

Modernizing security systems within aging infrastructure is no small undertaking. Therefore, if you've been called upon to do so, it is likely because a new or evolving risk has been identified. This could be increased security incidents, changing regulatory requirements, operational vulnerabilities, or other security risks.

Many times, an internal risk assessment can help identify these risks and their potential impact. This allows for a more precise, data-driven approach when determining where upgrades are most needed. In one example, a large school district underwent an independent risk assessment, revealing that 30-40% of its 4,000-5,000 cameras were non-functional. Many of those that remained had issues such as blurred images and obstructions. Additionally, their legacy DVR systems could only support 16 cameras per unit, capping the coverage far below what was needed.

Based on these findings, it was clear that new technology investments and system upgrades were required to reduce risk. From there, the district and key stakeholders could estimate budget, create a timeline, and prioritize implementation phases based on the most critical vulnerabilities.

Ultimately, the district replaced faulty cameras, filled coverage gaps, and upgraded to an enterprise-level solution, enabling remote monitoring and centralized health checks across all schools district-wide.

Approach to Best Practices

Engaging with Stakeholders

A strong project plan will also reveal which stakeholders require engagement. Identifying the right stakeholders early is critical to the success of any modernization project.

Stakeholders could include those within the organization (IT, finance, communications, legal, or facilities departments), external partners (systems integrators, consultants, or regulatory agencies), and those who are ultimately impacted by the system itself (students, teachers, parents, or administrators).

Often, key stakeholders are unaware that they are key stakeholders. For example, the network team may control infrastructure elements, such as switches and cabling, that are essential for security system upgrades. Without their buy-in and coordination, critical steps such as pulling new cable or upgrading bandwidth could become major roadblocks.

How To Determine Which Stakeholders Require Engagement

Map out all the groups or individuals:

Look for those who own or manage related infrastructure, have a budgetary role, are responsible for compliance, and/or will use, maintain, or be impacted by the system.

Ask, "Who can say no?"

Identify anyone who could delay, alter, or potentially prevent the project.

Look beyond obvious titles

Sometimes the most significant stakeholders aren't those at the top of the organizational chart, like facilities managers who control wiring closets or communications teams who need to know about emergency notifications.



Approach to Best Practices

Conduct early discovery meetings

Ask leadership, "Who else should be involved?" and, "Who owns or touches the systems, processes, or physical areas being upgraded?"

Document stakeholder roles

Not all stakeholders are the same. Some will approve funding, some will provide technical input, and some just need to be kept informed.

Communicate the project as a shared mission

Make it clear early on that this isn't just "security's project". It's a campus-wide initiative tied to shared goals like safety, security, compliance, and efficiency.

Once stakeholders have been identified, it's important to determine how to engage with them.

Each set of stakeholders brings its own unique mindsets, schedules, and priorities. Understanding their perspectives helps avoid unnecessary pitfalls while creating strong partnerships that ultimately impact the project's success.

For example, IT departments often protect sensitive information, while network and communications teams may be equally protective of their systems and infrastructure. Involving these groups early, sharing information, and demonstrating how the project aligns with their objectives can help build trust and foster cooperation.

You will also need to tailor your communications to the stakeholder group you are hoping to engage with. Some teams prefer to communicate via email, while others prefer to do so in person. Some teams need frequent engagement, others only once. Some teams require detailed technical information to stay engaged, while others prefer high-level updates that focus on outcomes.

Understanding these preferences early helps prevent miscommunication and ensures that each stakeholder group remains actively invested.

Approach to Best Practices

Adding Contingencies

With a plan in place and stakeholders outlined, it is now time to think through and create contingencies. These alternative plans address the inevitable challenges that could, can, and will arise.

For example, what are the risks if a camera system fails in a legacy environment? In this case, an entire building or the entire school may need to be shut down. An appropriate contingency plan might involve temporary measures to maintain operations. This could include the deployment of security personnel, the installation of temporary surveillance cameras, or the utilization of remote monitoring services. The key is to prevent unacceptable outcomes by having a plan B and C (at least up to two degrees) ready until the full issue can be resolved.

Contingencies can be financial, operational, and even political. Financial contingencies are standard practice, such as adding a 10–15% buffer to budgets to account for unforeseen expenses.

Operational contingencies include practical solutions that keep systems and operations running when unexpected challenges occur. Political contingencies help manage stakeholder expectations and maintain trust when things do not go as planned.

Contingencies are not necessarily shared with stakeholders at the outset, but should be prepared in advance so you can respond quickly and decisively when issues arise. Offering various solutions, including less-than-ideal options, is essential so risks are clearly understood and unrealistic ideas are ruled out early.

Ultimately, contingency planning reduces risk, strengthens your credibility with stakeholders, and ensures that unexpected obstacles don't derail the entire project.

If adding contingencies, managing stakeholder relations, and creating a plan sounds like a significant undertaking, that's because it is. This is where the value of a project manager, program manager, or consultant becomes clear.

Addressing Legacy Challenges with Modernization Best Practices

The challenges facing legacy educational environments can generally be divided into three categories: Environmental, Technical, and Operational.

While it would be impossible to cover every conceivable challenge you may face when implementing modern security solutions alongside aging infrastructure, this guide seeks to highlight key best practices and strategies for overcoming common hurdles.

And because every educational environment is different, you should consider these best practices in the context of your facilities and adjust your plan as needed.

Environmental

Environmental challenges refer to the physical conditions of the facility or facilities where the new or revised system is installed. These include factors such as building age, environmental hazards, historical designation, and accuracy of plans

Challenge: Age of Facility

Many school facilities were constructed long before modern security, electrical, network, and IT infrastructure standards existed. Outdated construction methods or materials (such as stone) also may not support new technologies without significant modification. This can lead to complications regarding the physical installation of hardware and additional costs to modernize the building itself.

Best Practices

Conduct surveys to identify the existing infrastructure's ability to support modern technologies. This includes evaluating power availability, network cabling, wall and ceiling composition, and physical access for installation. Where older materials or layouts pose challenges, consider low-impact or wireless solutions that minimize the need for structural modification.

Addressing Legacy Challenges with Modernization Best Practices

Challenge: Environmental Hazards

Many potential environmental hazards lie in older facilities, particularly those built before the 1980s. Some hazards, such as the use of lead-based paint, may already be known and documented.

In contrast, others, such as mold and the presence of rodents, may only become apparent during system renovation or installation. Exposure to these materials can pose serious health risks to workers and building occupants, trigger costly remediation projects, and delay project timelines.

Best Practices

Addressing environmental hazards demands strict adherence to environmental safety standards and best practices. Institutions should never attempt to manage hazardous materials in-house or cut corners by hiring unlicensed contractors. Instead, hire certified and licensed environmental firms to engage in hazard identification, removal, and remediation. Potential downtime should also be factored into project schedules. In many cases, work may need to be delayed until summer breaks when the facility can be safely closed.

Challenge: Historical Designation

Hundreds of U.S. schools and universities have buildings listed on the National Register of Historic Places (NRHP). The [Secretary of the Interior's Standards for the Treatment of Historic Properties](#) offers guidance for modifying such properties, allowing for necessary modifications to meet current needs while also preserving the building's historical character. Historical designation further complicates security modernization projects, as any proposed changes must often go through multiple layers of review and approval.



Addressing Legacy Challenges with Modernization Best Practices

Best Practices

The best way to address historical designation challenges is to engage with stakeholder groups early and often. This could involve communicating with internal architectural review groups, local historical societies, and state preservation offices. These groups will outline necessary guidelines for any proposed changes. In some cases, it may be necessary to customize security systems to blend seamlessly with the property's historical features. Custom solutions can help meet security needs without compromising the historic nature of the property.

Challenge: Accuracy of Plans

Many older schools face challenges with the accuracy of their existing drawings and floor plans.

In many cases, original blueprints are outdated, inaccurate, or completely absent. Any renovations and updates made to facilities may also not be reflected in the given plans. A lack of accurate plans leads to difficulties when pricing designs or estimating the scope of work for security system installations.

Best Practices

In cases where the existing drawings are insufficient or absent, thorough on-site assessments are critical. This allows the team to gather real-world data and confirm the layout of the building and any critical infrastructure.

A professional drafting firm can also conduct these assessments, providing accurate, up-to-date drawings of the entire building. In the short term, accurate plans eliminate potential rework and reduce the risk of mistakes during the design and implementation phases. In the long term, these updated plans serve as a valuable resource for ongoing building maintenance, emergency planning, and future upgrades.

Addressing Legacy Challenges with Modernization Best Practices

Technical

Technical challenges refer to the associated requirements and limitations of the installed systems, as dictated by the current infrastructure. This includes aging cabling and infrastructure, lifecycle management, programming and configuration, and network and power limitations.

Challenge: Aging Cabling Infrastructure, Conduits & Pathways

Older schools and universities were often constructed when the leading technology was telephone lines and copper cable. Today's technologies, such as OSDP standards, facial recognition devices, and Power over Ethernet (PoE+), enable more secure and efficient security systems; however, existing infrastructure often struggles to support these newer technologies.

Furthermore, older buildings were not designed with modern technology requirements in mind. As a result, they usually have limited space for adding new wiring or expanding existing conduit systems.

Best Practices

Start by communicating early and clearly with stakeholders about the limitations of the building's infrastructure. Present them with options that balance function, aesthetics, and cost so they can make informed decisions. Then, work closely with said stakeholders to design cabling pathways that meet the discussed requirements. This could include expanding existing pathways, utilizing concealed conduits, or deploying wireless technologies where appropriate.

Challenge: Lifecycle Management

The challenge with older school buildings is that they were designed for the 'right now'. From design to materials, those who built the school and installed original systems may not have considered how the school would grow and change. Don't fall into the same trap with the type of technology you select for your security system. It's critical to consider the technology's full lifecycle, from planning to installation, preventative maintenance, and eventual replacement.

Addressing Legacy Challenges with Modernization Best Practices

Best Practices

Don't treat your system's storage needs, network capacity, and cybersecurity requirements as a baseline or afterthought. Building flexibility into your design today will help ensure the system can evolve with the institution's needs over time.

Lifecycle management also means acknowledging the reality that device hardware typically has limited manufacturer support periods. Many systems are supported under standard maintenance programs for approximately seven years, after which they transition into "long-term support" phases, offering only critical cybersecurity patches. Planning for regular assessments, phased upgrades, and eventual system refreshes is essential to maintaining security effectiveness over time.

Challenge: Programming & Configuration Standards

As systems become more complex and projects grow to involve multiple rooms, buildings, and even separate schools, inconsistencies in programming and configuration can create significant challenges. Without clear standards, issues such as mismatched camera settings, inconsistent device naming, and miscommunications can arise. For example, two different schools in the same district could have cameras configured with different resolutions or with completely different naming conventions, making system management confusing.

Best Practices

Establish and enforce a standardized programming and configuration framework from the outset. This ensures that devices are consistently set up with uniform naming conventions, resolution settings, and system parameters regardless of the location or number of stakeholders involved. These standards should be well-documented and shared, while regular audits during the deployment phase can help catch inconsistencies early.



Addressing Legacy Challenges with Modernization Best Practices

Challenge: Network & Bandwidth Limitations

Modern security devices often require network connectivity and power, or Power over Ethernet (PoE) to operate. However, many facilities still rely on older cabling that cannot support the bandwidth or power demands of new technologies. Legacy networks often max out at 1 Gbps, which can quickly become a bottleneck when adding high-capacity devices. Beyond bandwidth, physical limitations such as insufficient switch ports, outdated cable grades, and limited PoE capacity also present challenges.

Best Practices

Remember that bandwidth is a finite resource. Every device on the network consumes part of the available data throughput. That is why it's critical to involve IT and communications teams from the outset of a project. Defining expectations around network use, port requirements, and system compatibility ensures that the security solution can be supported within the organization's broader IT framework. Planning for future expansion also helps prevent the need for costly network overhauls later.

Operational

Operational challenges are the most difficult to define, as they vary widely depending on the project or system type, environment size, stakeholders involved, and organizational culture. Operational challenges include divergent stakeholder priorities, creating feedback loops, resource limitations, and compliance requirements.

Challenge: Divergent Stakeholder Priorities

Deploying a new or upgraded security system involves multiple stakeholders, and it's crucial to understand their unique priorities. This is how you gain buy-in: by ensuring each group sees how the project addresses their specific needs and concerns. Facilities teams may prioritize ease of maintenance; IT departments may focus on cybersecurity and integration into existing networks; security teams may seek to enhance incident response capabilities; and finance may focus on cost control and ROI. Even external priorities from parents and students have a place in shaping expectations for security modernization.

Addressing Legacy Challenges with Modernization Best Practices

Best Practices

Refer back to the stakeholder mapping and engagement best practices previously outlined to ensure all relevant parties remain engaged throughout the project lifecycle. Open, early communication helps uncover each stakeholder's priorities, enabling you to design a system that balances diverse needs. This approach fosters trust and facilitates cross-departmental support when additional resources are needed. Know that you can't please everyone, but a collaborative approach to problem-solving, where all stakeholders' concerns are acknowledged and addressed, can prevent costly delays.

Challenge: Creating a Feedback Loop

Without a structured way to capture and learn from past issues, teams are likely to encounter the same challenges in the future. The same could be said for the project's successes. The security modernization you are undergoing today will likely need to be modernized again in just a few decades, if not sooner. Having a feedback loop in place helps ensure that systems and teams know what worked and what didn't last time.

Best Practices

There are many ways to create an effective feedback loop. One option is to conduct a stakeholder roundtable after every project phase, conduct post-project interviews, or create an accessible feedback form where stakeholders can submit anonymous feedback. Creating a feedback loop doesn't always require formal processes either. It can be achieved through cultivating relationships and fostering a culture of continuous learning. Regardless, it's important to encourage an open and transparent communication culture where feedback is not only accepted but actively sought out.

Addressing Legacy Challenges with Modernization Best Practices

Challenge: Resource Limitations

Resource limitations are by far the most common challenge faced by security teams when trying to modernize existing systems. Public K-12 schools are no strangers to small budgets, while higher education institutions often require greater investments due to their sheer size. Money, time, personnel, and equipment are all finite resources that the organization must carefully allocate. These constraints can create significant challenges, as teams may struggle to prioritize which needs are most critical and which can be deferred. Often, the pressure to do more with less can lead to trade-offs that compromise the effectiveness of security measures.

Best Practices

Overcoming resource limitations is a matter of creativity, compromise, and value engineering. Value engineering involves prioritizing investments based on the greatest security needs and operational value, while finding ways to reduce costs without sacrificing security outcomes. For example, consider leveraging existing infrastructure while upgrading only critical components. Lastly, explore government grants and funding programs available to K-12 and higher education institutions for security improvements. These resources can help ease budget constraints and support costly infrastructure upgrades.

Challenge: Compliance Requirements

One factor that can't be creatively managed or overlooked is the legal constraints that must be adhered to in system modernization. This could include contractual obligations with vendors, service providers, and stakeholders, as well as applicable laws, industry standards, and privacy regulations. Consider the [Jeanne Clery Act](#), a consumer protection law that requires colleges and universities receiving federal funding to disseminate a public annual security report (ASR) to employees and students each year, to include statistics on campus crime and details about efforts to improve campus safety.

Best Practices

Compliance is a non-negotiable when it comes to security. Failure to comply with such regulations can lead to legal consequences, financial penalties, and operational delays, potentially jeopardizing the project's success. Therefore, it is the responsibility of all stakeholders to ensure that all regulatory and contractual obligations are met throughout the process. This can be accomplished internally by internal legal departments and compliance teams or externally by third-party consultants.



Deriving Additional Value

With best practices outlined and plans in place, you're ready to start the security modernization process at your school or higher education facility. But the story doesn't end there. To truly maximize the value of your investment, it's important to consider the ongoing strategies and approaches that can enhance the effectiveness of your project. Consider them the cherry on top that could make a good school security modernization project great.



Proactive & Reactive Documentation

Proactive documentation asks you to document things such as project approvals or budget cuts. You may not need them, but by documenting these elements in advance, you create a clear record that helps guide the project and reduces potential misunderstandings. It's also just as important to document reactively, storing product manuals, recording camera configurations, and documenting negative stakeholder feedback. This documentation helps you solve current problems and allows you to refine processes that prevent recurring issues – an invaluable tool your future self (or future security teams) will thank you for.

Strong Stakeholder Relationships

Building strong, trust-based relationships with stakeholders is key to the success of any security modernization project. Trust is built when you take the time to explain risks and provide solutions rather than simply pointing out problems. Explaining the “why” (a potential health or safety risk) instead of just focusing on the “what” (an increased timeline or budget) helps stakeholders understand the broader implications of decisions and creates a collaborative atmosphere. The value here lasts long after the modernization project is over. You've made a valuable ally within the educational organization that you may need to call upon again in the future.

Quick Success Factors

Another way to win stakeholder trust? Demonstrate quick wins. Like IT projects, security success often starts with a proof of concept. Instead of pushing for large-scale commitments from the start, look for immediate, smaller successes that demonstrate progress. This could involve something as simple as adjusting a few cameras to enhance the field of view or addressing inefficiencies in an existing security setup.



Deriving Additional Value

Other times, it's about building a solid business case, demonstrating return on investment (ROI), or fixing a broken internal process. These quick wins build trust with the team and set the stage for larger, more complex changes down the road.

Working with a Third Party

Several previously mentioned third-party services can help you and your teams successfully tackle security modernization in the education environment. Whether it's a grant writing service that helps secure additional funding, a security project manager that provides day-to-day project oversight, or a survey team that creates updated site drawings, third parties can fill in critical gaps. Security consultants, in particular, deliver exceptional value as they have experience working with security teams and stakeholders within an education-based organization.

Moreover, they've navigated similar projects across various learning environments, providing them with a practical understanding of security modernization projects. Their knowledge and skill set can save you valuable time, reduce costly mistakes, and help ensure your security efforts stay on track.

About Atriade

The best practices outlined here reflect the collective expertise and real-world experience of the Atriade team. Atriade is a trusted security consulting firm with decades of experience delivering tailored security solutions. We specialize in security system design for access control, perimeter protection, video surveillance, visitor management, and other advanced physical security technologies. Our expertise extends beyond system design to include security master planning, program development, risk assessments, professional services, and end-to-end project management.

For over 20 years, we have partnered with Fortune 50 companies, universities, and K-12 schools to help them navigate complex security challenges with a strategic, forward-thinking approach.



How Atriade Supports Your Education Security Goals



Reasons to consider Atriade for your K-12 or higher education security modernization project:

- Let us serve as your project manager, providing day-to-day oversight, coordinating stakeholders and vendors, and managing communications so you can focus on securing your school.
- We'll conduct a thorough risk assessment, identify areas for improvement, and create an actionable plan for system deployment, taking into account applicable budgets and timelines.
- Tap into our deep understanding of educational environments and security technologies, where we tailor solutions to align with your academic calendar, operational constraints, and campus culture.
- Gain access to proven tools and processes, from documentation templates to risk assessments that have helped other districts and institutions successfully modernize their security posture.
- Trust a partner who's done it before and seen it all, so we can create contingencies and proactive strategies that minimize disruption.
- Partner with trusted, certified third-party suppliers with specialized expertise and proven solutions in their respective fields.
- Connect with Atriade today to explore how we can help transform your educational institution's security infrastructure.

Learn More: atriade.com/

Contact Us: atriade.com/contact-us/

Connect: www.linkedin.com/company/atriade

