Guidepost

FUTURE-PROOF YOUR SECURITY DESIGN THROUGH A HOLISTIC APPROACH

WHAT IS FUTURE-PROOFING?

According to Wikipedia, future-proofing "is the process of anticipating the future and developing methods of minimizing the effects of shocks and stresses of future events."

What is future-proofing in terms of security programs? Future-proofing means approaching the design and operational elements of your security infrastructure in a way that allows it to evolve and keep pace with the shifting threat landscape while addressing ongoing business requirements.

When applied from a holistic standpoint – intersecting operations, technology and the built environment – future-proofing will help you plan for the long term and lessen the impact of such change.

OPERATIONS MUST DRIVE TECHNOLOGY

When approaching your security design project, it is important to look beyond the technology and review the overall operations of your business, its needs, the programmatic aspects, and the built environment. *Technology should be driven by operations and business needs — not the other way around. Instead of trying to understand where technology is going, focus on how technology is impacting your employees and your goals.* For instance, does your business culture, technology deployment, and security goals support the use of a mobile device credential in lieu of an access card for opening doors?

With your goals in mind, you can take the steps necessary to create a security program that can scale appropriately to the changes in the business and threat environment. Technology can be used to support your overarching goal.

CHANGE IS COMING – READY OR NOT

The requirements to provide safe and secure environments for work, the education sector, special events, critical infrastructure, and public venues have changed. We have an obligation to understand the risks and act on these changes, and we need to bake this into our design programming in a proactive manner. Security is often overlooked at the beginning of the design process and not integrated early enough in the design discussion. All aspects of design and operations impact safety and security from site selection to the guard services contract.

Think about the education sector. Traditionally, schools have been built with a focus on the educational experience. Large, bright windows are important in schools to offer natural light and connectivity to the outside environment. This design feature needs to align with the need to provide a safe and secure environment. The security of the outside environment now has to be taken into consideration and the "Open Campus" design concept has safety issues. Schools are seeing the need to integrate safety and security early on, making it a design priority, while still allowing for an excellent education experience. The goals are not mutually exclusive, but require discussion and creativity to resolve, which is best done through design intent with all parties participating.

Not planning for a changing security environment can be seen in airports throughout the country. The Transportation Security Administration (TSA) screening is often a retrofit solution into a space that did not anticipate the mandated 1973 process. Today, newer or remodeled airports have been able to take the required program needs and incorporate design early to create the proper space to support the program. Has your building lobby been designed to support a screening process or turnstiles? Does the physical space support the operational requirements?

5G network infrastructure is coming and will provide the ability to connect more wireless devices at once. It's going to have a substantial impact on smart device and Internet of Things (IoT) technology, which in turn will peripherally impact architectural design and construction. 5G will bring opportunities and challenges. The higher-frequency transmissions won't pass through certain building materials well, resulting in the need to consider better ways to deliver signals. Devices that currently must be hardwired won't need to be. It will be paramount to identify the management of people and IoT early on because this will change how a security program uses technology.

FUTURE-PROOF TO HELP STRIKE BALANCE

Future-proofing keeps us nimble so that we can make changes and adapt when a threat arises – it can help strike a balance between your operational/business needs and your safety/security needs. Consider the following takeaways:

1. **Weigh business needs against those of the environment**. This is not just about the due diligence of safety and security; this is about business needs and people working effectively. If getting to work is stressful or employees feel unsafe in their work environment, then this is not conducive to an effective workspace. If the recent incidents of school shootings worry students and teachers, then this is not favorable for their education.
2. **Don't layer tech on top of tech**. Take the technology and apply it in a manner that makes sense for your business. Don't default to layering technology on top of technology to address problems. Rather, ensure the technology's backbone supports your program and safety and security needs in an efficient and productive manner, while adapting to changes in technology.
3. **Prepare to pivot.** Whatever the disruptive technology or world event might be, it may dramatically change the way we work and the way we interact every day. It's going to impact the infrastructure of what we design and these changes

> may have unintended consequences. How do we anticipate and apply changes in a way that allows us to be resilient and mitigate risk in our ever-changing world? It’s a challenging feat. But, by committing to a holistic approach we can change and adapt to those circumstances, in a way that keeps us safe and secure and allows our programs and businesses to work successfully.

At the end of the day, we are never able to completely predict or anticipate all the technical and societal changes ahead, but it is imperative that we keep a sharp eye on the horizon to future-proof — to create state of the art security programs that can flex as changes occur and allow for continuous improvement.