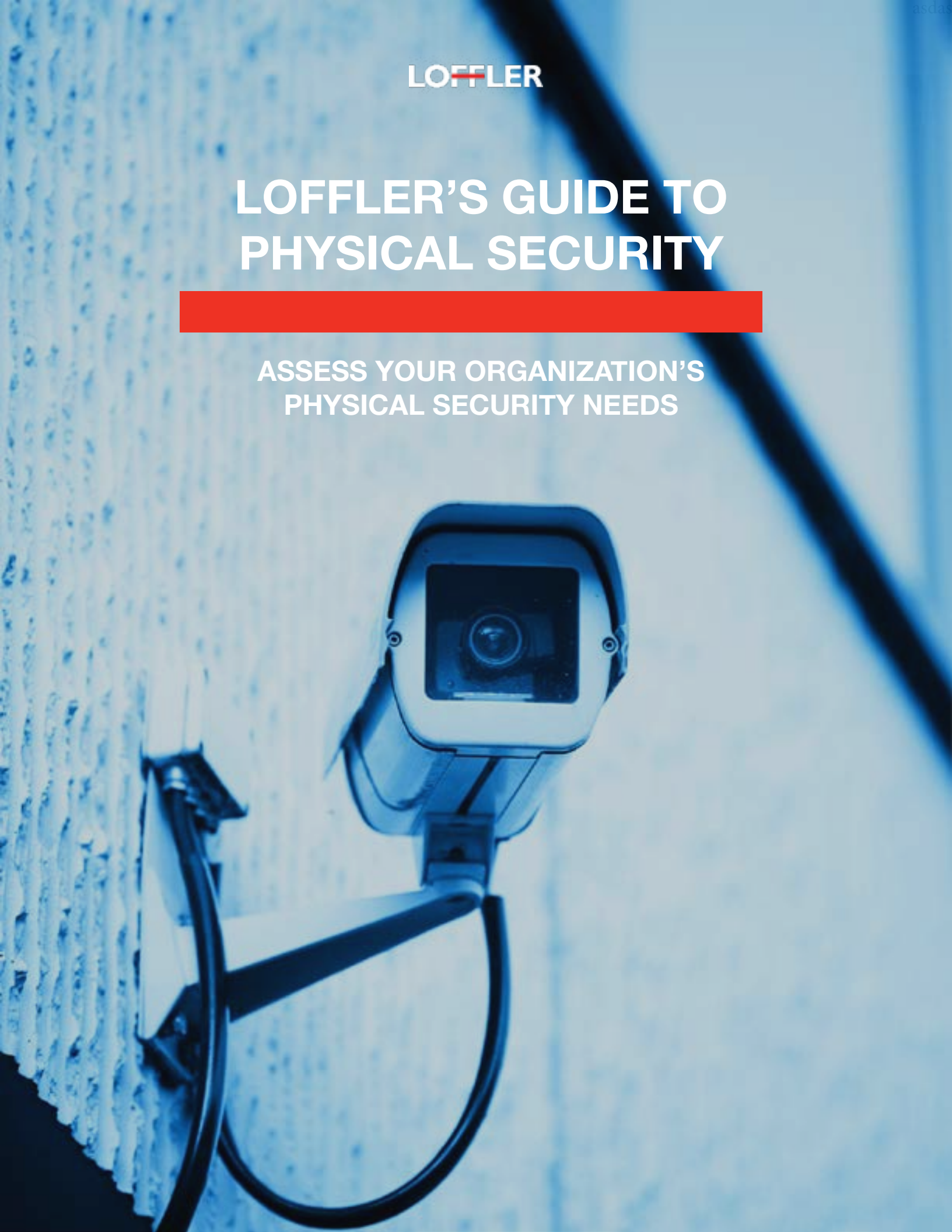
LOFFLER

LOFFLER'S GUIDE TO PHYSICAL SECURITY

ASSESS YOUR ORGANIZATION'S PHYSICAL SECURITY NEEDS



CONTENTS

Every business organization should have a reliable physical security system tailored to their unique needs.

Having a reliable physical security system is an integral part of business success. In a world of constant digital transformation and evolving capabilities, information and data are constantly at risk. A solid physical security structure in will help you maintain and grow the trust and confidence you have built with employees, customers, and organizations you serve.

Physical Security is designed to protect the assets and facilities of your organization using physical measures. Throughout this workbook we will help you to get a better understanding of the vital pieces of Physical Security as well as how to best assess your current situation as well as determining what you may need.

What is Physical Security?

Physical security is oftentimes thought of as security guards, secure entry systems, sign-in sheets, etc. Though these are all viable and relevant components to a businesses' protection, in our present-day digital world, physical security has grown to encompass so much more. Security today is not a "set it and forget it" type of situation it is an vital business practice that requires constant attention and awareness of ever-emerging threats. Physical security refers to the protection of the data, software, hardware, networks, and software from physical activity that potentially cause massive damage or loss. All of the top firewalls and cybersecurity measures in the world won't provide much attention if a trespasser can simply walk into the server room without cause and exit unnoticed with a company computer or other valuable asset.

One of the biggest mistakes businesses make in regards to physical security is focusing on the outer perimeters or Web-based walls while neglecting the importance of internal structures. Physical attacks can affect a business from many angles such as entering into a secure data center, using equipment without authorization, or accessing restricted areas of a building, all of which are physical security issues. These intruders can easily destroy IT assets, steal information through USB ports or even upload malware onto business systems, or they can walk away with merchandise, business property or hard copies of important documents.

LOFFLER

PLANNING YOUR PHYSICAL SECURITY UPGRADE

Identify your current problems and goals

Your organization is only as safe as its least secure asset. It's important to take a deep dive into your infrastructure and find potential bottlenecks. Outlining your current security will help you strategically plan a system that works now and in the future. Are you looking to improve safety measures? Wanting to align your security operations with certain strategic goals? How effective are your current security methods in comparison to where you would like to be?

Create a Baseline of Operations

Are you aware of how each of your departments work together to provide a layered level of security? Which department(s) manage access control? Are all employees aware of security protocols? Who is in charge of making sure protocols are followed and equipment is functioning properly?
Does your business hand out keys to contract cleaners who enter the building after hours and those transactions time-stamped and recorded? What procedures do you have in place to retrieve keys and access materials once employees are terminated or resign from their position? Take time to consider the security incidents and potential costs that could be avoided with a more secure and reliable system in place.

Work with an experienced Physical Security provider

Security experts can help make planning, implementing and maintenance a pleasant experience. Cookie cutter systems are no longer sufficient. Your provider should work with you through each and every strep of your physical security update to help you find solutions that meet your unique needs. It is crucial that the provider you choose knows how to plan and implement a system that communicates with your current IT environment.

Access Control

Access control is a phrase most people have heard one time or another, but how does this relate to physical security? In simple terms, access control is about keeping people out of places they don't belong, but it also provides a number of other benefits. Having a reliable access control system in place allows owners to easily revoke or provide access for individuals with a simple click of a button on their cellphone. Door locks, lights and HVAC systems can be programmed; this provides business owners with piece of mind and the added benefit of reducing operational costs.

Do you have multiple campuses or office buildings? Your access control system allows for simplified multi-location admittance making it easier for managers and employees who travel from one to the other while tracking who and when someone is accessing the facility. In the event of an emergency or potential threat, access points can be locked quickly, preventing theft or harm of employees and structures. The need for a strong access control system seems like a no-brainer, but where do you begin and what makes sense for your business?

Read on…

TYPES OF ACCESS CONTROL

Do you need to restrict access to your entire building or just limit accessibility to certain areas? Admittance to a business is no longer simply controlled by a receptionist at the front desk or security guard at the door. Access is tracked and controlled with three main security methods each becoming increasingly more stringent: what you have, what you know, and who you are.

WHAT YOU HAVE

This level of security entails something you know in your physical possession such as a key, swipe card or FOB.
Though the least expensive, it is also the least reliable. There is no guarantee the access token is being used by the right person; physical tokens are easily shared, stolen, left unattended or lost and used by someone else.

WHAT YOU KNOW

Instead of relying on a physical object, some businesses opt for a “keyless” method in which a password or code, that only specific individuals know is used to gain access to a specific area. This system is more reliable than a swipe card or key, but passwords can easily be shared or stolen, especially if they are written down somewhere that others can access them.

WHO YOU ARE

This method relies on the recognition of unique physical characteristics to gain entry, often called biometrics. Biometric scanning devices verify identity by scanning faces, eyes or fingertips.
Biometrics is most often implemented in the innermost layer of your security system in conjunction with another ID method such as a pin code or password. Biometric security is very reliable.

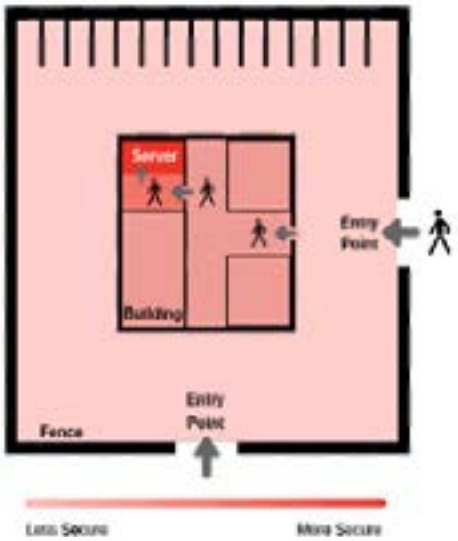
What level of Access Control do you need?

In creating a strong, reliable access control system first map out your facility, even a simple sketch will do. Identify the areas and entry points that will need varying levels of security; where are the areas that potential threats could enter your building? Through this mapping exercise you will be able to begin building a layered security system that is cost-effective, non-intrusive and more secure. This sketch will naturally help you implement a “depth of security” where access methods become increasingly stringent as you approach the most information-sensitive areas of your building.

Combining different identification methods increases reliability at each advancement towards sensitive information. For example, a business may require the following sequence of access control points as someone moves throughout their facility:

1) A card swipe to gain entry onto the main grounds
2) A code or password to enter the brick-and-mortar building
3) A password AND biometricsto be allowed access to the server room

Depth of Security



The sequence of these security methods increases dependability at each entry point. The server room, where the most sensitive information is housed, is protected not only by its own secure access but also by each access point implemented along the way.

The perfect access control system for your organization strategically balances the system costs and nuisance factor of your security measures against the risk of the wrong people having access to business-critical areas. Designing a security system is a complicated art which is why we recommend you work with a security partner that knows how to layer security technologies to give you the most protection. In short, you know who needs access to what areas; we know how to make it happen.

Cloud Based Video Surveillance

Traditionally, video surveillance systems are actively monitored by security personnel to identify potential threats on screen. In the past some utilized video cameras connected to unreliable VHS recorders that were viewed only in the instance of a security breach. Modern day surveillance security uses intelligent software the is able to detect threats on its own. Once identified, the technology has the capability to notify human security personnel or appropriate authorities to take action. Reliable, up-to-date video surveillance has the potential to maximize the security level for the business itself and also provides peace of mind for employees and customers who frequent your facility.

Using a cloud or hybrid cloud video surveillance system allows for secure remote access to surveillance information, that which is live or that which has been recorded and stored. Security control gives you the flexibility to connect with other building access and management systems, while operating them without having to step foot on the property. Cloud-based video surveillance is cost effective with its predictable monthly cost and provides businesses a strong overall network.

Advantages of Video Surveillance Systems

• 24/7 Secure Mobile Access

Updating your security cameras allows you to have the latest and greatest in technology advancements. You will be able to securely access video feeds from anywhere using your desktop computer, a smart TV, mobile device, etc.

• Improve General Business Operations

New cameras can allow for positive changes, even with simple tasks such as when an overhead door is left open, or lights have been left on after hours, you will now be aware of every situation and be able to immediately make corrections.

• Theft prevention

Many small businesses can lose close to $50K due to vandalism, break-ins and even intellectual and company property theft. Cameras placed throughout the business help deter both internal and external criminals from following through on any potential criminal plans.

• Prevent Sexual Harassment

The US EEOC and FEPA received nearly 10,000 charges claiming sexual harassment in the workplace in 2020 – even in a pandemic year when many individuals were working remotely. Implementing CCTV cameras throughout your business serves as a deterrent to this type of activity and provides employees an increased sense of security. If a litigation does ever occur, the surveillance video can help to formulate the appropriate response.

Is Video Surveillance feasible for my small business?

Absolutely! In the past, small business surveillance methods have been costly and time consuming. Upkeep and staffing limitations have made it difficult for small businesses to acquire reliable, quality video security systems. Historically, low-cost options have provided low-quality video, insufficient storage, lack of mobile access and analytics, limited user control and the tendency to quickly become outdated. Small and medium businesses (SMBs) need a video surveillance system that is: simple, affordable, secure, and accessible. The cloud-based video surveillance systems meet these needs and more, making them an attractive, cost-effective option.

Cloud-based surveillance is an option many SMBs have not yet considered due to the false belief that cloud technology is outside their scope. The fact that cloud security offers mobile access to video systems without the need to be physically maintained makes cloud surveillance something all businesses should consider. This updated form of video surveillance allows business owners to monitor happenings via mobile application or web browser. There is no longer a need to rush to the physical location at the sound of an alarm or suspicious activity, your camera footage is constantly at your fingertips with the cloud.

Old, clunky video systems quickly lag behind and are often operating with outdated software and firmware, making them very unreliable. Both the camera and the software require constant updating. When using the cloud, updates to both software and firmware are done automatically giving you surveillance that is always current. This system also provides SMBs with analytics, video management and improved monitoring which typically isn't included in the basic video systems.

Cost is understandably a big concern for SMBs and the cloud is a predictable, affordable option. Cloud video surveillance usually entails a subscription which, for businesses, means cost control. Considering the cost of equipment and software you would buy for an on-location traditional video system, you will spend less upfront and the same (or less) over time on a cloud subscription. In addition, the need to hire someone to continually maintain your surveillance system is eliminated.

Operational Efficiency with your Physical Security System

> Physical security is the protection of business property and personnel from physical actions and events that could cause serious loss or damage.

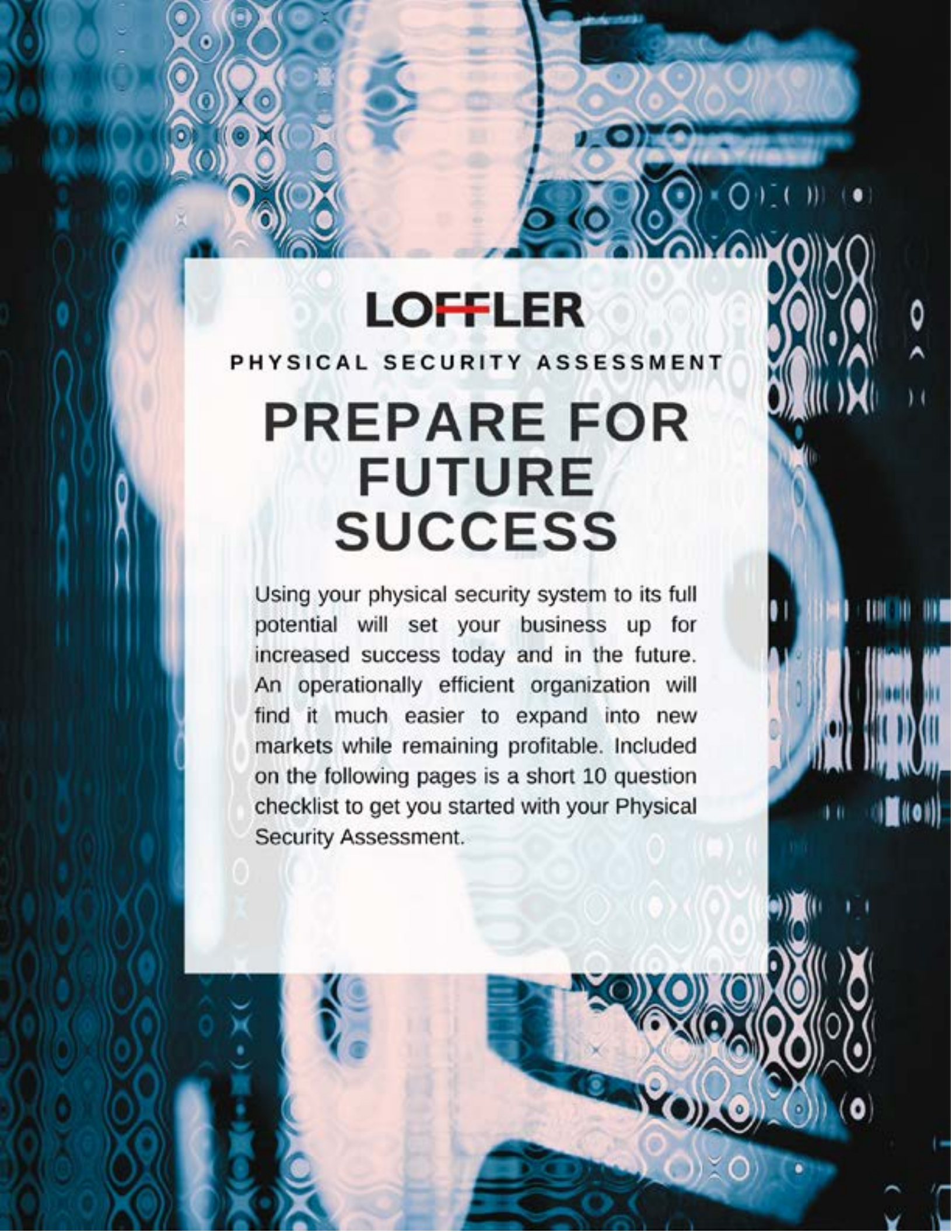
Once you have come up with an overall security goal you hope to achieve, it is important to look at how these systematic changes will affect your business. Incorporating real-time notifications through video surveillance and access control along with inventory tracking built into your security system will create a winning situation: optimal output for your business and exemplary service for your customers.

Check out this example: say a customer walks into a section of your building or store, a notification is triggered to notify employees on their mobile device that a person has entered into a specific area. The employee now has the opportunity to engage with customers and offer help to make sure they're finding what they need.

Data-Driven Insights and Analytics

Using RFID tags in your physical security system makes it easier to gather transaction data that many departments in your organization can analyze. Your marketing team can use this information to understand the performance of specific campaigns, pinpoint ideal customer demographics, predict trends and plan future initiatives. Your physical security system can also help with asset management, production tracking, shipping/receiving and service and warranty authorizations.

Achieving operational efficiency with security technology isn't only specific to the retail industry. Manufacturers can use tracking solutions, such as RFID, in production processes to gain real-time visibility of project progress. The logistics and transportation industry is beginning to take advantage of this technology to connect with their database in order to track origins, destinations and identify materials being shipped.



LOFFLER

PHYSICAL SECURITY ASSESSMENT

PREPARE FOR FUTURE SUCCESS

Using your physical security system to its full potential will set your business up for increased success today and in the future. An operationally efficient organization will find it much easier to expand into new markets while remaining profitable. Included on the following pages is a short 10 question checklist to get you started with your Physical Security Assessment.

CHECKLIST

		Yes	No
1	Are all business access points monitored either manually or electronically?		
2	Is employee building access restricted to controlled entrances?		
3	Are keys and FOBs signed out to employees or contractors with facility access?		
4	Is access to restricted areas monitored and reviewed?		
5	Do you check access control, surveillance and lighting systems regularly?		
6	Is your current surveillance system up-to-date and in working condition?		
7	Are yor outside perimeters within view of surveillance equipment?		
8	Are stairwells and other access points monitored by surveillance cameras?		
9	Is there someone designated to receive notifications when suspicious activity is detected?		
10	Are all employee aware of security protocols and access restrictions?		

LOFFLER

You're Done!

What now? You've done the hard work of assessing where your current physical security needs may be, now choose a partner to show you options that will fit those needs.

Save this PDF with your responses to your desktop now. Then click "Submit" and to send to a Loffler team member for next steps.

Submit Your Workbook

MN: Bloomington; Duluth; Mankato; Rochester; St Cloud; Willmar; Grand Rapids | WI: Eau Claire; Hudson; La Crosse; Green Bay
IA: Sioux City; Spencer | NE: Norfolk | ND: Fargo; Grand Forks | SD: Aberdeen; Sioux Falls

Helping You Succeed