THE POST-COVID WORKPLACE ACCESS CONTROL CHECKLIST

Office managers are tasked not only with managing the day-to-day operations of their company's workplace, they're also challenged with safeguarding and securing it. In a post-Covid workplace, maintaining a safe environment gets even more challenging. That's a lot to think about, because there are many variables to consider, often dependent upon the office configuration and purpose.

Choosing the security approach best suited for a particular office depends upon its size, location, risk level, hours of operation and addressing other vulnerabilities -- especially minimizing germ sharing. By taking inventory of these factors, office managers and HR leaders can evaluate the best security system components to implement. Among the most important decisions is deciding which elements need to be included when evaluating office needs. It can help to think about physical security modularly and break it down into the following parts:

☐ Fire Alarms

Fire alarms are an essential part of workplace safety but are often part of a building / property responsibility. If you own your own building, you'll want to make sure this is covered.

☐ Video Surveillance

Video is becoming a critical component of a modern physical security system. It provides additional insight with "visual intelligence" to support the ongoing processes involved in securing people, equipment or intellectual property. It can also provide historical event verification if there is a potential need to pull video footage after an event occurs.

☐ Visitor Management Systems

A fundamental condition of a secure office is knowing who comes and goes, and if they are authorized to be there. While access control (see next topic) manages regular staff occupancy, visitor management is required for outside individuals who need to temporarily enter an office for meetings, consulting assignments or for maintenance.

☐ Access Control

This is the cornerstone of any physical security package and controls who has access rights using a card, key fob or mobile phone app to get into an office space or building. It is a central feature at one of the highest-touch, shared office workspaces, the entrance. It is also tied to the alarm system to notify administrators when unauthorized access may occur. Having an unreliable access control system is keeps an office manager up at night.

Because access control is so crucial to office security and can most readily impact screening and contact tracing for potential Covid 19 infection, we will focus this discussion here. There's a lot to consider, especially when considering:

- Which system will be the most effective and reliable?
- Which security dealer or integrator will properly install it?
- Who will manage its ongoing operation, maintenance and alarm monitoring?
- How to respond to emergency breach situations?
- How can it help screen out potentially infected individuals from entering and/or trace their contact interactions should an infected occupant be identified after having been on-premise?
- **How can it help support a germ-free workplace?**

Unfortunately, while office leaders may know their security goals, they're not typically the best person to execute -- after all, they are not necessarily security experts. Many are not prepared with the expertise needed to choose and invest in an access control system best suited to their workplace.

If you're an office manager, and this strikes a chord, read on. We at Kastle Systems, the leader in managed security, are here to help inform you on all aspects of your physical security program and have summarized a few access control pointers to help you along the way.

PART 1: Space & User Requirements

Access control systems are developed to address specific security concerns, so it's important to first define who and/or what you are protecting, and what you're protecting them from, before selecting a product, vendor or methodology. That way, you can determine the system parameters that best meet your needs.

These are the types of questions you should consider:

- ☐ How many points of public access are there? Should each public access point have the same level of access and restriction?
- ☐ Which solution would best suit your office, workers and visitors– individual office door locks, a stand-alone keypad, or a complete electronic access control system?
  - » Standard manual door-lock hardware, which is an inexpensive option initially, requires ongoing physical "key management" and may require replacement if keys are lost or stolen.
  - » **Keypads are very affordable and easy to implement, but in a post-Covid world, are extremely unsanitary being potentially touched by everyone daily**. Also, former staff can access the office using their old code unless you remember to deactivate it.
  - » A complete electronic access control system can allow varying levels and times for access to spaces, based on individual identity giving office managers more control over their environment. **These platforms can also more readily accommodate mobile-based, touchless access credentials with automated doors which can be a powerful benefit in the prevention of contagion spread**.
- ☐ What kind of access credential should be used? How easy is it to use? What level of encryption for the is necessary to ensure the office is safeguarded?
  - » Metal keys are easy to copy, be lost or be forgotten.
  - » Standard 125 kHz Prox card technology is widely used and affordable, but it can be easily hacked. Card credentials also require that the office manager keeps an up-to-date account of all cards in and out of use. **Also like a keypad, cards and swipe-readers are extremely unsanitary**.
  - » New cloud-based systems that are mobile-enabled – where the credential is issued via an app on the user's smartphone -- can send encrypted access signals via Bluetooth or NFC are quite secure from copy or hacking. **They can be operated hands-free, so are more sanitary and potentially more conducive to a post-Covid workplace**. Mobile credentials are growing in popularity for their user and administrator convenience.
- ☐ Can you encourage social distancing by setting up separate dedicated entry doors and exit doors to prevent cross flow or traffic and avoid close contact between occupants?
  - » Separate ingress and egress make it easier to designate a directional flow within the office.
  - » With separate access readers at each entry/exit, you can develop a daily record for each occupant's presence within the office, and all those who were there simultaneously, making contact tracing, in case of and individual being diagnosed as infected, a much quicker and easier process.
- ☐ How will the system be monitored? Will you do it yourself and be on call after hours, have dedicated security staff with designated workspace in your office or would it be more efficient and/or cost effective to outsource to a third-party monitoring company? **Who will be available in the event of work-from-home mandates (like our recent one) in the future?**

- ☐ Do you need to manage your access control system from outside of the office? You may want to consider a cloud-based platform that can be accessed from anywhere online to open doors, revoke access rights, monitor activity, and even lockdown entire spaces. **These systems have proven invaluable for administrators working remotely during this time of office space closures**.
- ☐ What will be the plan and policy when an employee leaves the organization? Is it typically the office manager's responsibility to collect all the issued keys or key cards from a departing worker or change access codes? Do you want to consider integrating your HR employee database with the access control system? More advanced solutions like Kastle's sync access rights directly with the HRIS employee database directory allowing HR/IT managers to turn off an access credential's operation automatically, so it just stops the worker's access immediately.

PART 2: Integration Considerations

Whether you're inheriting a pre-existing access control system or starting from scratch, it's important to consider how all the components of your solution will work together. Office managers often struggle with how best to integrate their office's security technology with individual employee technology.

To help ensure your systems work in unison, keep these questions in mind and don't be afraid to pose them to your vendors:

- ☐ How integrated should the access control system be with identity management? If the access identity directory can integrate with the HRIS database, enrolling or revoking access rights driven by employee hiring or termination is simultaneous – one automatic action makes it easy and quick which could be critical in the case of a disgruntled employee.
- ☐ Can the system seamlessly integrate with Covid 19 screening procedures and results if necessary, to efficiently operationalize access rights based on individual test results each day to ensure potentially infected individual's access credentials will not allow them entry until they are symptom-free?
- ☐ Will individual access activity be recorded electronically, and, if so, how will the data be stored and backed-up? Many organizations require regular audits of access history – this could be particularly important in the case of infected employee or visitor (ex. contact tracking presence of a coronavirus carrier and any staff with whom they interacted) or an undetected theft.
    - » Can you monitor janitorial staff access after hours to ensure they are spending an adequate amount of time to deep-clean your spaces to minimize potential exposure to infection?
- ☐ Is there an access control system used in your building lobby? If so, can that system accommodate your potentially different individual tenant access control technology in their spaces? Will staff have to carry two cards? This might force you to enroll and manage two separate staff access directories. Advanced providers, especially cloud-based providers like Kastle, can integrate directories across platforms to provide a more seamless user and administrator experience with only one credential to use and one database to manage.
- ☐ Do you want your system to integrate with a video surveillance platform? With video that's integrated with access control, you can view the cause of any intrusion immediately rather than looking at recordings after the fact. You can also use it to confirm potential contact occurrences between individuals on premise should the need for contact tracing arise if an Covid-infected occupant is identified.
- ☐ How will visitors or temporary staff be granted access to your workplace? How will you know they are approved to enter and when? How will the access scheduling, credentialing, and monitoring sync to ensure your space remains secure from unwelcome entrants? Also, how can you ensure that your visitor is only given access after having cleared Covid-screening protocol? Having Access Control that integrates with a robust Visitor Management system is an important consideration.
- ☐ Can the integration be used to trigger automated tasks like audits of staff attendance and space use recording? This can be a requirement for many firms, especially when doing government contracting work.
- ☐ Do you need an open application programming interface (API)? This would allow your access credentials to operate with other smart office building technologies like smart elevators or dynamic HVAC systems. (This could enable

touchless elevators with your access credential if you have an provider with advanced open-standard technology like Kastle). While many providers boast an open API, which makes integration with other technologies possible, they don't always share enough data points to allow for an effective integration. Be sure to explore this with the security vendor(s) you consider. The Kastle access control platform has an open API, so integrating with other building management platforms becomes easier to manage.

- ☐ Flexibility is key. Does your solution need to accommodate mobile access that can grant or deny entry across multiple spaces? Depending on your provider, this can be designed into the system using mobile device-based credential. The ability to deny access rights quickly can be useful if an individual is identified as a virus carrier or if your office staff are forced to work-from-home and you need to ensure they do not attempt to access the office.

PART 3: Future Proofing

Access control technology involves sophisticated equipment and complex software that needs to be regularly updated as developers make upgrades and improvements. To help ensure your workspace stays secure, it's important that your system is "future-proof" – that the operation continues to work the way you want for the lifetime of your space and can evolve with advances in technology without having to replace the hardware. Do you and/or your staff want to keep your system up to date yourselves or would you prefer that software update be pushed automatically from a cloud-based provider? Consider these issues before you purchase a system that might be outdated in a few years.

PART 4: Management and Maintenance:

Once you've decided on a well-designed system from a top-notch access control vendor, most of the actual access control user experience has yet to occur. The day-to-day monitoring, management and maintenance of your access control is just as important to consider as the system you purchase.

Keep these points in mind:

- ☐ Who will monitor the system? What are your staffing needs, the hours of operation and the backup contingencies, should issues such as a power outage, or a quarantine (like the COVID 19 mandated work-from home situation) arise?
- ☐ Will the access control vendor host in-person, on-site training for your staff? Will they return for new staff training in the future? Do they charge for ongoing training?
- ☐ What maintenance or service agreements will be put in place for your access control systems? A system must be regularly tested, and non-operating devices must be repaired. Can your staff do it themselves or should you outsource to experts? Will they be available in the event of an office shut down as with the coronavirus? Security monitoring providers, like Kastle's Managed Security service, are deemed "essential services" and will always be on-call, even in times of quarantine.
- ☐ Will the access control software be periodically updated and who is responsible for timely updates – your staff, the manufacturer or service/security integrator vendor?
- ☐ If your security procedures change, who will help you reassess the access control plan for gaps?

It's critically important to choose a security provider that does more than install access control hardware and software, but who also acts as a strategic partner to help ensure your system stays at optimal performance long after the initial installation.

There is much to consider when implementing security for your office. If you're feeling overwhelmed by all the possibilities, give Kastle Systems a call. This is what we do. We are a managed security service provider which means we don't just sell a system – we are partners with our customer for the long-term from design to installation, monitoring, service, updates and maintenance. We are security experts with the most advanced technology in the industry and almost 50 years of innovation in physical security.

We'll be happy to walk your space and provide a complimentary assessment to help you determine the best long-term solution for you, your staff and your office.

WWW.KASTLE.COM 855.527.8531 INFO@KASTLE.COM

KASTLE SYSTEMS