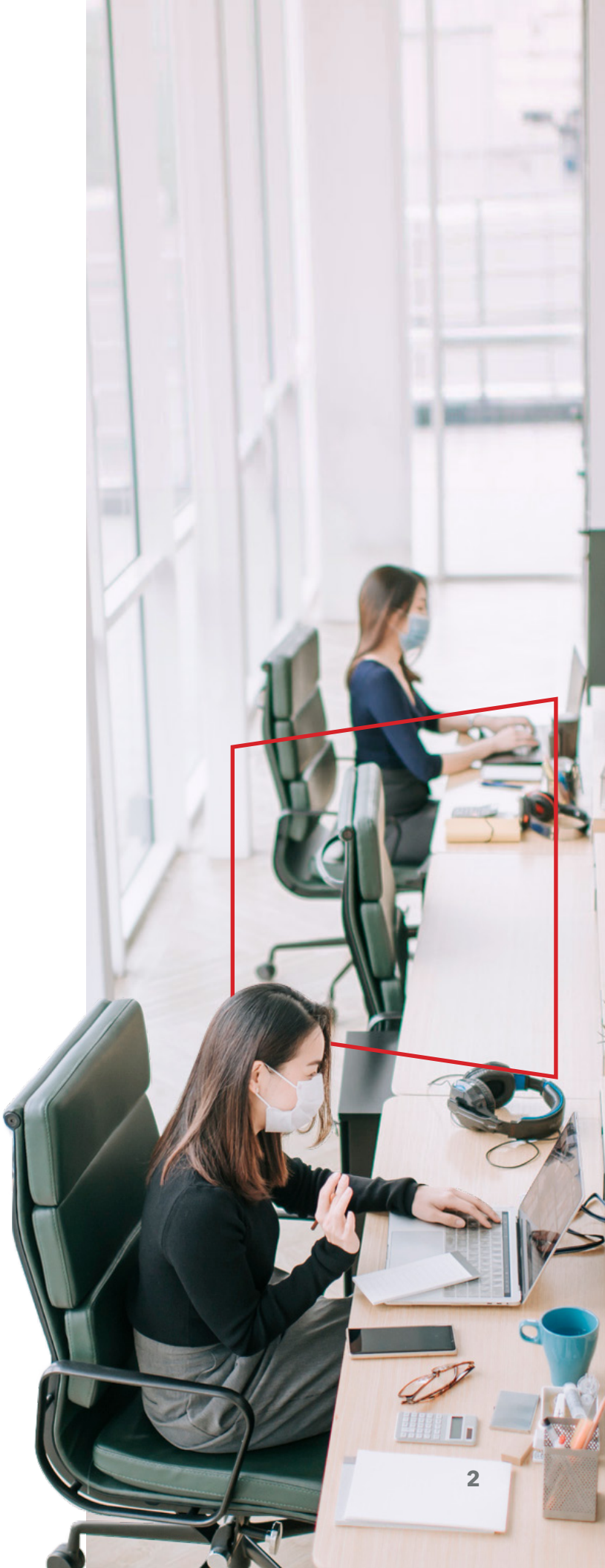
STAYING SAFE IN THE NEW NORMAL

KASTLE

Due to ongoing concerns about COVID-19 and its variants, the wholesale return of employees to offices has been delayed. But many companies are taking a proactive approach to manage protocols so some level of normalcy can be maintained during and after the transition. Business leaders are altering policies around things like social distancing and other health-related measures, scheduling, and data and personnel security. Company leaders and HR managers must effectively communicate these changes to workers to ensure new processes are understood and adhered to.

Security measures, in particular, are essential because everyone has a role to play in preventing bad actors from taking advantage of this transitional time to enter company premises and harm employees or get their hands on sensitive data. Physical threats can have an impact far beyond the immediate danger, and data breaches can cause untold damage to a company's reputation and cost endless hours and dollars in trying to regain access or recreate records.

As your company grapples with what the next normal may look like, you may be working in an unresolved state with ad-hoc hybrid working situations. That's all the more reason to communicate early and often, so employees understand both temporary and permanent changes such as updated rules or how to operate new technology. We've created this handy reference guide to help you prepare for those conversations and address any questions that arise.



UNDERSCORE THE IMPORTANCE OF **SECURITY**

No business wants to think about threats to the personal safety of its employees. However – though unlikely – workplace attacks are possible, and companies must do everything they can to prevent them. You can use statistics to drive home the fact that such unimaginable incidents can and do happen. For example, the U.S. Bureau of Labor Statistics reports that nearly 21,000 people in private industry in the U.S. experienced intentional injury by another person in 2019 (the most recent year for which data are available). You can research similar facts pertinent to your specific industry and business type.

Data security may seem less personally threatening, but you can remind employees that any breach could very well impact their livelihoods. Due to the costs of rebuilding operations and the reputational damage resulting in lost business, many companies that are victims of cybercrime end up severely cutting back on their number of employees or even going out of business.

Brook Carlon, Chief Human Resources Officer at Kastle, noted, "The main point to drive home is that both physical and data security are highly relevant to employees, and each can have tremendous negative impacts." Therefore, all team members have a stake in following appropriate protocols to keep everyone safe.

"The main point to drive home is that both physical and data security are highly relevant to employees, and each can have tremendous negative impacts."

Brook Carlon, Chief Human Resources Officer, Kastle

MAKE IT **PERSONAL**

As we have just seen, employees can become the victims of physical and cyber attacks, but the good news is there is much they can do to help prevent them. As they return to work, team members can be trained in security methods, such as those listed here:

PHYSICAL SECURITY

- Using mobile credentials that cannot be copied or shared as can RFID cards
- Using access systems synced to an active user directory human resources information system (HRIS) so access can be denied immediately to fired or disgruntled staff members
- Refraining from letting anyone unfamiliar into the building
- Reporting suspicious behavior on the part of customers, vendors, or visitors
- Being aware of and cooperating with company policies and systems in place
- Ensuring procedures for regular security software upgrades and ongoing hardware maintenance
- Syncing video surveillance with access to verify the actual entrant matches with presented credentials
- Creating strict policies about which individuals are allowed to be in certain places at specific times and implementing real-time alerts for when the wrong person is in the wrong place at the wrong time

CYBER SECURITY

- Using strong passwords and two-factor authentication
- Using secure password management tools and avoiding the placement of passwords in obvious places, such as on sticky notes under desks
- Refraining from clicking on links from unknown email senders
- Reporting suspicious emails or activity
- Keeping electronic devices locked when not in use
- Using only secure networks to perform work
- Using cloud-based access control and video surveillance to remove the threat of hacking the onsite network from that system
- Allowing minimal access privileges to server areas

Because human error is to blame for many physical and cyber intrusions, companies must reduce their chances by providing robust and repeated training to employees. Carlon suggested, "To get more buy-in, remind them that just one mistake can cause major problems, and no one wants to be the one that caused the problem or be the person to blame. So, being well informed is in their best interest."

> "To get more buy-in, remind them that just one mistake can cause major problems, and no one wants to be the one that caused the problem or be the person to blame. So, being well informed is in their best interest."
>
> **Brook Carlon, Chief Human Resources Officer, Kastle**

IDENTIFY THE PROBLEM AND INTRODUCE THE **SOLUTION**

Once you have offered the background of worst-case scenarios and the fact that everyone has a part to play in preventing them, you can start explaining the specific security needs of your company. When employees understand why new technologies and processes are necessary, they're more likely to cooperate with solutions to help address the issue.

For example, maybe an understanding of new cyber threats (the problem) has prompted your IT department to upgrade software security (the solution). As a result, employees must now take different steps to access platforms and applications. Or perhaps the new hybrid workplace arrangements (the problem) have introduced the need for a more robust video surveillance system to help with contact tracing (the solution). As a result, employees must be included in videos and provide personal information.

In such situations, you can offer workshops on how the new system works and the expectations of each employee. Carlon stated, "Modern security technologies, including those provided by Kastle Systems, feature options like smartphone-based access control, cloud-based software, and integrated visitor management schedules." When providing information to employees, be sure to let them know how each of these features is helping to keep them safe.

"Modern security technologies, including those provided by Kastle Systems, feature options like smartphone-based access control, cloud-based software, and integrated visitor management schedules."

Brook Carlon, Chief Human Resources Officer, Kastle

PROVIDE APPROPRIATE **TRAINING**

After sharing the broad brushstrokes of the problem and how you have decided to address it, you should provide the appropriate training to set employees up for success in contributing to the solution. Such training may include one or more of the following:

Workshops that offer a chance to learn critical information, practice new skills, and get questions answered. For example, you could walk team members through the app, such as those offered by Kastle, that is now used to access the building and enter health information to help prevent the spread of COVID-19.

Online modules that enable employees to pursue training as they have time. These teaching tools should include quizzes that help to gauge team member's understanding of the new material.

Practice opportunities such as phishing simulations that can be implemented to determine how well workers can spot suspicious emails.

Within any of these formats, it's crucial to provide a picture of "before" and "after." That is, describe the current situation and expectations, then contrast how the new system differs. Another critical component is documentation that team members can refer to as needed. Consider implementing a "security" section on your intranet that provides videos, instruction manuals, practice opportunities, and quizzes.

You may even want to institute regular testing to keep workers up to speed on current practices.

Follow up with contact information so team members can figure out what to do if unsure, and reminders at meetings, in newsletters, and with signage around the office. Because of the importance of this information, don't worry about mentioning it too often.

ANTICIPATE AND ADDRESS **EMPLOYEE CONCERNS**

Communication about security issues is sure to bring up concerns, especially physical security. Some team members, including those who may have experienced a workplace threat in the past, may feel you're not doing enough to keep them safe. Others may feel that you're going overboard, that too much is being asked of them to maintain security, and that you are violating their privacy. All of these concerns are valid, and it's important to anticipate them as well as others that might come up, creating talk tracks for specific situations.

You must also be open to concerns you may not have anticipated and have ways of managing them. Here are a few tips for being prepared:

Have a predefined chain of command in place and communicate it to all employees. For example, they might be encouraged to first go to their direct supervisor, who might direct them to the department head if they cannot address the concern. Your HR department should be included as well.

Encourage employees to be specific about their concerns, and ideally format their inquiry as follows: "I've noticed X and am concerned because I'm afraid it could lead to outcome Y." Additionally, encourage them to have a solution in mind. Some concerns may be easily accommodated with just one conversation.

Take every concern seriously, even if it initially seems extreme. Remember that employees have had various life experiences, and they may have a unique response to a situation that others may not even think about. Carlon recommended, "Try to understand specifically how the issue impacts them personally and the company as a whole."

Exercise compassion. Some employees may have had experiences with workplace violence and become triggered upon hearing it discussed. Ask HR for tips on signs to watch for and have resources, such as therapist referrals, available if needed.

REWARD **COMPLIANCE**

After training, create a baseline of how knowledgeable team members are about the new technology, systems, or processes. You can accomplish this task through testing or creating reports in the automated access system or video camera footage. For example, you might watch to see how many people are holding the door for others, allowing them to enter the building without presenting their credentials. Carlon stated, "This step isn't meant to seek out those who aren't following the rules. Rather, it's a way of taking the current temperature of the situation to see where you might need to provide additional information or support."

Create a goal and give employees a reward when it's reached. One hundred percent compliance on credential presentation might be too high a bar at first, but you can make it 80% and then increase to 85%, 90%, and so on over time. Rewards can include things like parties, gift cards, or time off. Consider making it a team effort and rewarding the group with the best performance. With the group method, team members will likely encourage each other to perform as you've requested.

Keep employees informed of company-wide progress with updates on community platforms or via regular newsletters. As new processes become more habitual, it may be tempting to dial back on such methods. But keeping up with them, even if less frequently, is an excellent way to build security into the company culture and ensure that new employees understand its importance within their position.

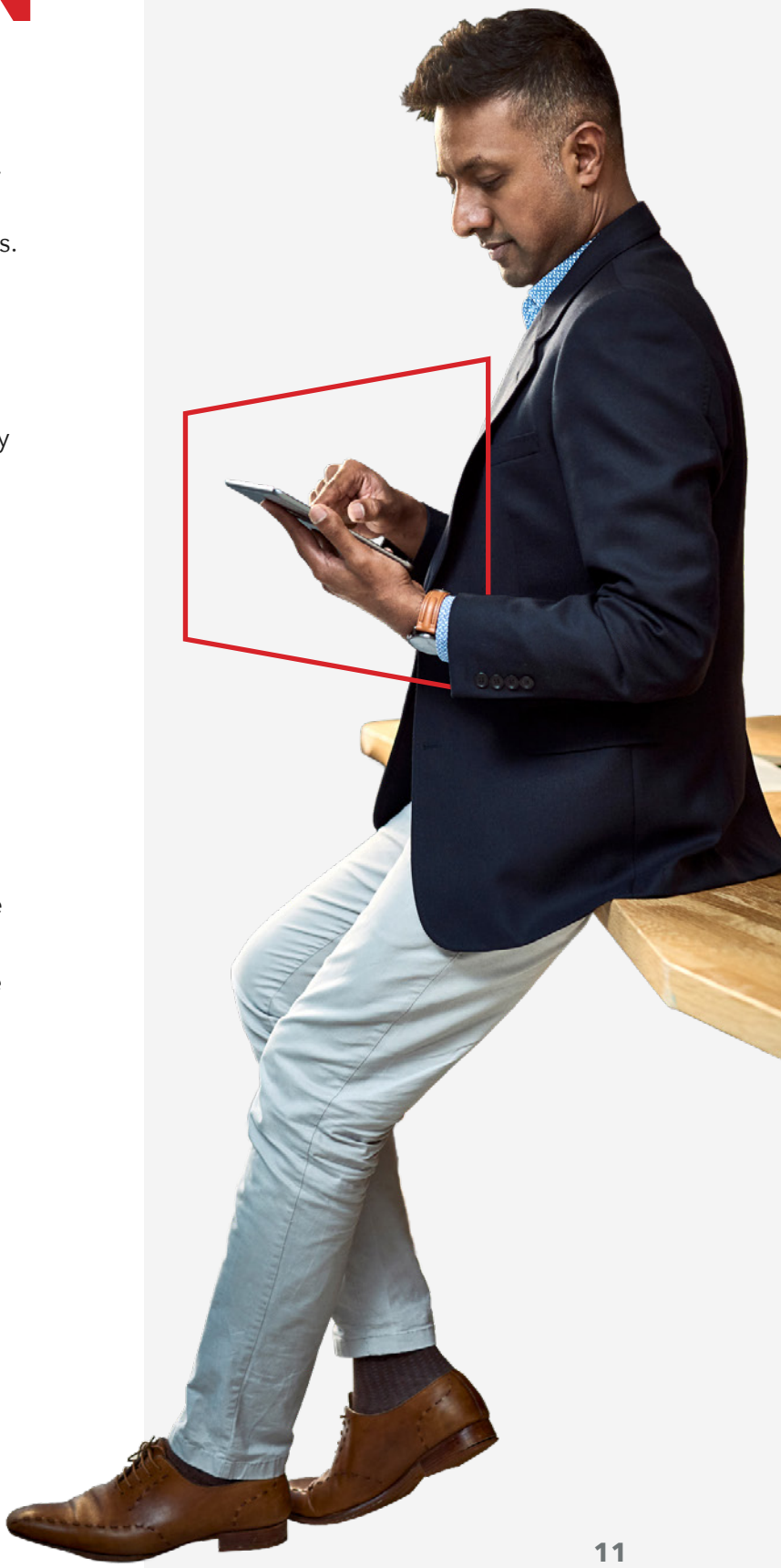
CONCLUSION

Security is on the list of the many things companies have reexamined since early 2020. Kastle has been privileged to work with many of them on new security systems and protocols. We strive to achieve a vision of "exceptional spaces" for our customers so that their businesses are places that people want to be.

Our business office and enterprise technology have helped customers refresh outdated systems, create infrastructure for office moves and make security easier to manage. Our cloud-based technology features an open interface that enables us to integrate access and video systems across various platforms.

In addition to advanced technology, we offer a superior user experience with flexible design and a focus on innovation. Customers appreciate features like hands-free access control, instant credential assignment, remote management, easy reporting, and secure visitor management. Our Security as a Service offering enables us to address customer security needs with an end-to-end managed approach (see sidebar).

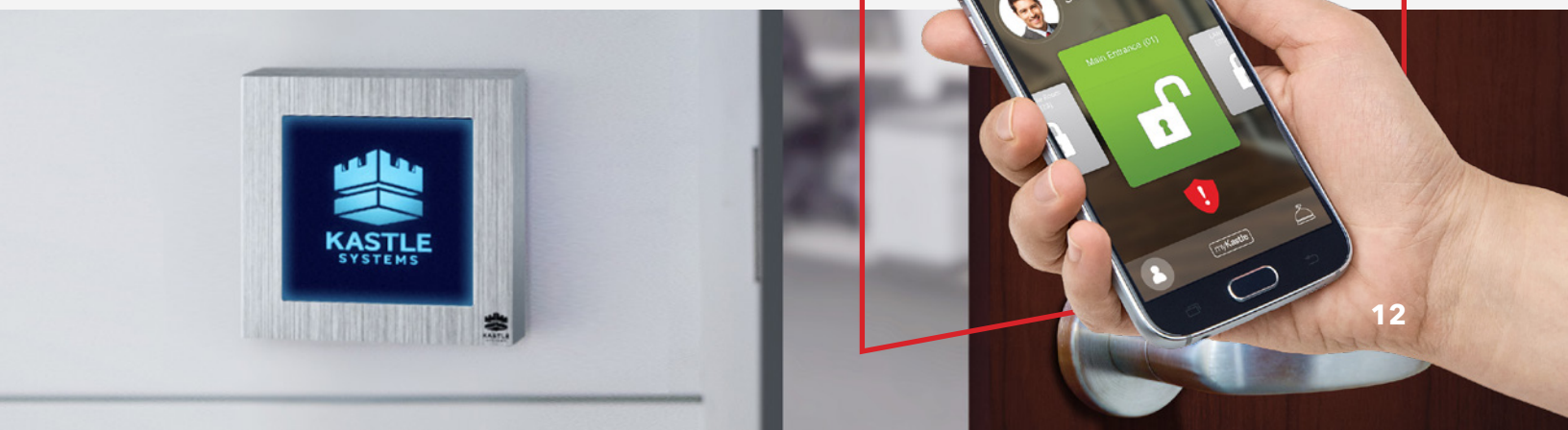
As employees return to work, the importance of clear communication about recent security changes cannot be overstated. Those that do it well will experience an enhanced sense of safety, greater worker buy-in, and, ultimately, higher levels of success.



UNPARALLELED SECURITY **MANAGEMENT**

Kastle is your trusted outsourced security partner. You can count on us to comprehensively address your security needs with our end-to-end managed approach:

- **Design.** We create managed security solutions based on an assessment of your unique environment.
- **Integrate.** We have open technology that easily configures to leading building system manufacturers so we can build standardized systems suited to you.
- **Install.** We implement our designs using industry best practices with minimal business interruption.
- **Maintain.** We repair, replace and warranty our products, including free ongoing software upgrades.
- **Monitor.** Working in the industry's most advanced operation centers, our team of specialists respond to critical signals that are reported to your administrators.
- **Protect.** We take responsibility for security procedures, database management, and reporting on trends and events, delivering the highest level of preparedness.
- **Support.** We provide dedicated account managers to work as your main point of contact while our tools and organization ensure we can always assist you quickly.
- **Safeguard.** We strengthen your business continuity plans with redundancy in power, connectivity, support coverage, and data storage.



KASTLE

HEADQUARTERS
6402 Arlington Boulevard
Falls Church, VA 22042

855.527.8531
info@kastle.com

License Number DCJS #11-2295

www.kastle.com