KEEPING STAFF AND CLIENTS SAFE AFTER COVID-19 SHELTER-IN-PLACE

By Rob Hammond, PSP, NICET III and Ryan Raskop, AIA, RCDD, NCARB, LEED AP

Salter

Introduction

The COVID-19 quarantine shelter-in-place has caused us all to learn different ways of being effective in our jobs. As a guide to using security systems to keep us safe when our businesses and offices reopen, this article discusses security technology as a "frictionless" way to control access to the worksite and minimize touching surfaces, evolving fever detection technology, and cybersecurity and how it affects physical security systems.

Part 1: Frictionless Access

When we return to our places of work, clients and staff will be concerned about their health. As businesses find ways to comply with mandates and allay people's fears, security technology can offer tools to help address these concerns.

One means of virus transmission is through touching surfaces; frictionless access to buildings will help address this concern. Touchless sensors for door operators allow a person to wave their hand near a sensor and have the door automatically open for them. This combined with touchless access control credentials will allow people to enter a building without touching the door or a card reader.

Optical turnstiles using touchless access control readers are an excellent way to quickly and reliably vet staff entering the work area. Combining these turnstiles with destination dispatch-type elevator systems allows staff to be vetted at the elevator lobby, granted access, and have their elevator car and work floor selected automatically. Staff can enter the building and go directly to their desk without the fear of touching infected surfaces.

Some companies are using a virtual credential that is electronically embedded in their employee's smartphone. The phone uses an encrypted wireless signal to a Bluetooth-enabled card reader, in the same way a card presented at the reader works. We then can email a link to download a secure credential to a person's smartphone. A contractor or new hire can receive an access control credential with no human contact, from the convenience of your laptop computer even if you are working from home. Card readers installed in the last several years might already have this Bluetooth feature.

Biometric access control devices also grant touchless access. An iris scanner uses an image of the eye's iris, which is like a fingerprint: no two are alike. The process is quick and does not require touching the sensor.

Facial recognition is another option. A camera takes a picture of your face, makes several geometric measurements, and compares it to a stored electronic template. Newer facial recognition technologies use near infrared (NIR) to scan a face. Rather than looking at the visible face, which an ordinary surveillance camera can see, the NIR sensor can scan the sub-dermal level to make spectroscopic measurements. NIR technology is proven, safe, and touchless.

There are many security technologies that can help people be and feel safe in this new environment. The technologies discussed here are just a few ideas that can help. To learn more about the many technology options available, use your favorite search engine or talk to a qualified and experienced security consultant to find and deploy these interesting technologies.

Part 2: Fever Detection

The first thing to understand about automatic fever detection systems is this is a fast-evolving emerging technology. Evolving technologies, in general, should be approached cautiously, as they are not well understood and their deployment can be problematic if not done properly. A few months ago, this technology was virtually unheard of. Today there are several companies competing with various strategies and levels of effectiveness. This paper doesn't endorse any product; instead, we will discuss, at a high level, the underlying technology and issues to be aware of when deploying fever detection products.

These devices use long-established technology to detect the infrared heat our bodies emit. Night vision goggles have used this technology for decades. Fever detection devices are not foolproof for three primary reasons: (1) as we know, a person can have the virus without symptoms or fever, (2) the system's reliability is greatly affected by how they are deployed, and (3) the effectiveness of the technology the manufacturer uses varies greatly.

Fever detection devices don't measure body temperature, they measure skin temperature, which can be at variance with body temperature. Skin temperature can be affected by things like exertion, coming from a hot or cold area, the type of lighting in the area, and recent consumption of alcohol. When fever detection sensors are used, expect false alarms and be prepared to offer secondary screening with medical-grade temperature sensors.

Look for detection systems that take the temperature at the inner eye. This is the most accurate location on the face, due to its proximity to the carotid artery. Sensors that read other portions of the face are generally not as reliable. There are international standards that address the technology and how to use this equipment. These standards address conditions such as the ambient temperature in the screening area and dictate that only one person be screened at a time. The person cannot be wearing a hat or glasses and cannot have hair near the eyes. The face must be parallel with the camera, the person cannot be sweating, and there should not be a bathroom or other water fixtures nearby because you don't want people splashing their face with cold water to deceive the camera's analytics.

Due to the urgency of this public health emergency, the FDA has suspended its requirement that these devices receive FDA 510(k) clearance, which is the certification required for medical grade devices in the U.S. The FDA also recommends that these devices be used only for triage and be paired with clinical-grade thermometers. Companies that are considering these devices should be aware that there are a lot of false claims in the market. They should research standards and seek guidance from organizations such as the FDA, ISO, and IEC before purchasing and deploying these devices. Security consultants are receiving a lot of requests from their clients to help deploy this technology and many of us in the security consulting community are quickly getting up to speed on this new technology and learning the best deployment practices.

Part 3: Cybersecurity

Although important before COVID-19, cybersecurity is now even more important as cyber-villains are more active. Security systems are especially vulnerable to attack because every device we attach to a network is a device that can be hacked. Today's surveillance cameras are powerful computers that have the same cyber vulnerabilities as a desktop computer.

One common and serious problem is that cameras and other devices are installed with their default password. There are specialized search engines that crawl through the internet looking for the address of all devices connected to the internet. "Smart" devices from cameras to refrigerators can be found with tools like this. Hackers use these tools to search for specific types of devices with known default passwords. They find their targets, use the default password, and plant their viruses.

Poorly secured security systems are not only vulnerable to hackers who might use cameras to spy on a home or facility; the hacker can also enter a security system and use it as a virtual backdoor to an organization's entire network. Your home router can also be found using these tools, so make sure you change all default passwords. Don't make your devices low-hanging fruit for hackers.

Another issue is email scams, such as a phishing attack where people receive an email warning they have been directly exposed to the coronavirus by a friend, colleague, or family member. The email advises clicking on a link for a form to fill out. To make the attack even more believable, it appears to come from a hospital. In the best of times, you should never click on a link or document from someone you don't know. Today, we need to be more cautious. Another scam comes courteous of the MUMMY SPIDER. This malware identifies email threads by subject line and formulates a reply to the thread. The recipients receive a message with a familiar subject line from someone they have recently corresponded with, increasing the likelihood that the recipient will open a malicious attachment.

Cybersecurity is constantly evolving and faces new threats every day. Now that many of us are working from home and using security systems remotely, there are new vulnerabilities that our IT professionals need to address. There are too many cyber-hygiene practices to address in this article, but having your security consultant working with IT professionals to protect your organization's physical and cybersecurity is a good first step.

About the Authors

Rob Hammond, PSP, NICET III is a security consultant for Salter. He has worked in the security industry for manufacturers, integrators, owners, and consultants. Early in his career, he deployed some of the industry's first access control systems. He specializes in security system integration, including access control, video surveillance, intrusion detection, and emergency communications. One of his roles at a leading security manufacturer was on a research and development team creating leading-edge security technology. Mr. Hammond's project experiences include corporate and educational campuses, office buildings, multi-family housing, emergency operations centers, hospitals, airports, government installations, research facilities, correctional institutions, power plants, and manufacturing plants.

Ryan Raskop, AIA, RCDD, NCARB, LEED AP is a Senior Associate at Salter, as well as a licensed architect and Registered Communications Distribution Designer specializing in building technology integration. Mr. Raskop brings over 10 years of experience and expertise in telecommunications infrastructure, electronic safety and security systems, audiovisual systems, and cellular network design. With his architecture background, knowledge of construction systems, and expertise in communications infrastructure, Mr. Raskop seamlessly integrates technology within buildings and their surrounding environments.