SIA REPORT:

SECURITY AFTER COVID

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org

Sponsored By
maize
marketing

A Message From Our Sponsor

In 2020, the COVID-19 virus spread across the globe. Governments, industries and businesses had to swiftly adjust to new safety mandates and figure out how to achieve business continuity during widespread lockdowns.

In the new SIA Report: Security After COVID, which is sponsored by Maize Marketing, the impact of the coronavirus pandemic on the security marketplace is discussed. This report takes gives us a closer look at the security industry's reaction, response and lasting changes of the COVID-19 pandemic.

Throughout the pandemic, the role of both security professionals and security technologies rapidly changed and expanded to aid with environment, health and safety objectives as well as virus mitigation. Temperature screenings, facial coverings, social distancing, and remote work became the new normal. New challenges arose such as increased cyber risks, greater network vulnerabilities, and lack of staffing due to the Great Resignation across the workforce. In response to these issues, businesses and governments turned to security technology to be a force multiplier. Touchless access control solutions, cloud-based apps, remote monitoring systems, and occupancy analytics all rose in popularity and have seen steady demand for long-term adoption. These are just some of the important topics that the report covers.

I encourage each of you to take a few minutes to read this report. Before we chart a course ahead, it is essential to reflect on the past. This helps to ensure we embrace key learnings that only come from evaluated, lived experiences. Ultimately, these lessons make us smarter security practitioners where we can truly have the greatest impact for our colleagues, partners and customers.

Thank you for reading and looking forward to a prosperous 2023.

Kevin Friedman
President of Maize Marketing, Inc.
www.maizemarketing.com

Introduction

In March 2020, security operations, along with everything else in the United States and the world, changed.

As the coronavirus spread, states of emergency were declared, lockdowns were imposed and social interactions were minimized. Economic activity plummeted, as people stayed home as much as possible, restaurants and movie theaters closed, sports leagues canceled games and video conferences replaced schools and offices.

For security practitioners and providers, risk calculations were adjusted, with threats now perceived to be coming not only from bad actors, but also from bad germs.

As places slowly reopened following the initial COVID-19 outbreak, many did so with new policies and procedures. Security personnel – and even some security technologies – took on new tasks related more to promoting life safety than deterring criminal activity.

During the next two years, society, to varying degrees in various places, adjusted to a new normal, one that commonly included mask-wearing requirements, occupancy limitations and other measures that often put security personnel in enforcement roles.

By early to mid-2022, with vaccines having been available for more than a year and pandemic fatigue running high, COVID mandates at all levels of government had largely been eliminated. Businesses and organizations that had overhauled their security to meet the exigent needs created by the pandemic now faced a new challenge – deciding which new health and safety-focused measures to keep while transitioning back to a non-pandemic posture.

Pandemic Changes

No matter the type of facility, operating under the threat of COVID often meant implementing a combination of procedures and technologies intended to mitigate the risk of virus spread. This was true throughout the country during the early weeks and months of the pandemic, but over time, regulatory requirements and market pressures came to vary widely among states and localities.

At sites where these changes were deployed, both security personnel and security devices had new roles assigned to them. The new measures included but were not limited to:

Health Screening

- Thermal cameras were deployed as temperature screening devices, but not without some controversy. While the Food and Drug Administration said that, "when used correctly, thermal imaging systems generally have been shown to accurately measure someone's surface skin temperature," attempts to use the cameras for screening crowds of people were not supported by the evidence. As the agency noted, "the systems have not been shown to be effective when used to take the temperature of multiple people at the same time. They should not be used for 'mass temperature screening.'" In addition, people infected with COVID-19 do not necessarily have high temperatures, and a high temperature does not necessarily mean that a person is infected.
- Other screening approaches included temperature taking using handheld devices, in some cases by security personnel, which required close contact that was inconsistent with social distancing recommendations; self-attestation regarding non-exposure to infected individuals and absence of symptoms; and proof of vaccination and/or a recent negative test.

Face Covering and Social Distancing Requirements

- With many locations enforcing indoor mask-wearing and social distancing and maximum occupancy requirements, video analytics were developed that could gauge compliance. Whether or not such technologies were used, enforcement required personal interaction, which created new difficulties for security personnel. As Bloomberg reported in March 2021, one year into the pandemic, "In the Covid era, guards are expected to act as public health officials, in addition to law enforcement, without having the authority and often the experience of either." Around the same time, an article in The Guardian cited multiple attacks on security personnel related to Covid rules and interviewed a guard in Oakland who said, "We get cussed out every day."
- Less controversial were measures aimed at optimizing the flow of people. Entry and egress points at many large facilities were drastically reduced, so that, instead of allowing people to come and go through multiple doors, there might be only one way in and out for visitors, with a separate entry and exit for employees.

Expanded Use of Security Technologies

- At the governmental level, The Guardian reported in April 2020 that, “The coronavirus pandemic has led to an unprecedented global surge in digital surveillance, researchers and privacy advocates around the world have said.” For businesses and organizations, meanwhile, video cameras and analytics offered life safety and compliance solutions through mask detection and occupancy and distance-monitoring analytics, in addition to their traditional security purposes. Also, remote access to video and other security systems supported the maintenance of a site’s security operations even when the availability of personnel was limited by illness, quarantine, resignation or other causes.

Increased Cybersecurity Demands

- With the massive expansion in the number of people working and learning remotely, maintaining secure computer systems became more complicated. Each new endpoint connected to, but not contained within, a site’s network added a new potential vulnerability during an already disruptive time when operations and budgets were facing unprecedented challenges. For organizations that did not have existing mobile work policies and network infrastructure, the threat could be even more serious, especially with physical security now so often converged with IT systems. As Interpol noted in August 2020, “With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.” And in May 2021, CBS reported that, “Cybercriminals ransomed millions of dollars from businesses during the COVID-19 pandemic, using time-tested tactics like phishing, social engineering and other hacker tools of the trade” and noted that “so-called ransomware-as-a-service is on the rise. Prior to the pandemic, criminals were forced to invest time and resources into investigating targets. Now cybercriminals can simply hire ransomware services on the dark web or buy the software to attack using email.”

> “
> **With organizations and businesses rapidly deploying remote systems and networks to support staff working from home, criminals are also taking advantage of increased security vulnerabilities to steal data, generate profits and cause disruption.”**
>
> *~Interpol*

Lasting Changes

Society's return to normal has happened at different speeds in different areas. Indeed, even as of August 2022, a few places in the United States still required masks.

For the most part, though, pandemic-specific countermeasures have been lifted at nearly all locations. That having been said, some practitioners have found that a few of the approaches implemented since 2020 remain beneficial, if only to be better prepared for the next biological threat.

"My opinion is that health issues within the facility should be another risk factor, and I believe some cities from around the country and the world are adopting this practice," a consultant to a mayor in one of the biggest cities in the United States said.

He added, though, that some of the solutions that were marketed during the pandemic proved to be disappointing, so addressing this additional risk factor could involve approaches not yet tried.

"During the start of COVID, many owner/operators were quickly adopting the technology to assess health risk from within the workplace," he noted. "However, the technology was immature and unreliable. This frustrated the users and I now see many buildings with the scanning kiosk stuck in a corner somewhere."

A security director for a large property development company said that the pandemic produced a change in mindset, and that locations are now preparing for contingencies that involve long-term interruptions to operations.

"Business continuity was the responsibility of an emergency manager with input from other departments, with a goal of sustaining operations for a short time frame, hours to a few days," he said. "Plans are now incorporating long-term solutions for extended business interruption."

A security official for a professional sports league, meanwhile, said that the mindset of customers has also changed, which demands a broader approach to safety and security, even in the absence of an ongoing pandemic.

"Guest and staff expectations about attending or working an event at a stadium have risen, so the stadium operators have to find new ways to earn the trust of the guests and staff while delivering a safe, secure and memorable experience," he said.

> **"**
>
> **...We're all having significant problems getting hourly event security employees and other departments to come in to work. So how can you use technology to reduce your manpower?"**

The lingering second and third-order effects of Covid are also influencing decisions about security. The pandemic cost millions of people their jobs, and many of those people appear to have decided not to return to work, resulting in what analysts have called The Great Resignation. This has had a significant impact on many security operations.

"We would love to leverage more technology and less people because of the manpower problem we're all having," a security official for a professional basketball team said. "I think every stadium and arena that I talk to around the country right now, we're all having significant problems getting hourly event security employees and other departments to come in to work. So how can you use technology to reduce your manpower? It's easy to say, 'Oh, we have all this stuff, you just use this technology rather than manpower.' But how can you really do that? We're trying to go through exercises

> **“The crisis on public transit systems threatens the nation’s recovery from the coronavirus pandemic.”**
> *~The New York Times*

of doing that now, how we can do things and still be comfortable with our security footprint.”

In addition, the homicide rate increased by nearly 30 percent from 2019 to 2020, while the violent crime rate, after a three-year decline, went up by almost 5 percent. A professor of criminology at Georgia State University told Politico in October 2021, “I’m not surprised at all that we had an increase in crime. Criminologists and public health people were saying that that was going to be the case as soon as they heard about the pandemic. And it’s pretty much come true at this point.”

Public transportation systems have been particularly hard hit, as a security expert in the transit community noted.

“Crime and disorder have increased at many transit agencies as has the number of persons experiencing homelessness taking shelter in stations and on trains and buses,” she said. “Assaults against transit employees have increased as well at some properties.”

This has put security operations at the forefront of efforts to restore ridership lost because of Covid. In April 2022, *The New York Times*, noting that transit crime rates have risen in several major cities, reported that, “The crisis on public transit systems threatens the nation’s recovery from the coronavirus pandemic.”

New York Mayor Eric Adams is looking to technology to enhance security on the city’s subways.

“We believe we have a technology that we can use in the subway system that many passengers are not even going to be aware that they are walking past – a device that could detect weapons,” he said on *MSNBC* in April 2022. “We are excited about the possibilities, and I’m not going to leave any legal technology off the table when it comes down to keeping New Yorkers safe.”

New York is already expanding surveillance on the subway, with one pilot program installing hidden video cameras on 100 subway cars, though they will only be used forensically, not monitored in real time.

Some security practitioners have found that procedural changes made in the name of health and safety are now contributing to smoother and more efficient operations, particularly in the area of entry and access control.

“One positive impact from changes in behaviors is that attendees are more familiar with fewer entry points because of the need for pandemic screening processes,” the deputy chief of police at a large university said in reference to sporting events. “Because of this, security officials should avoid reopening entryways that were decommissioned during the pandemic.”

A hospital security official, similarly, said, “We’re down to two entry points – one for both visitors and staff and one for just staff.”

“We participate more in screening of visitors than before,” he added. “We’re doing a better job of controlling access for both staff and visitors.”

Another person responsible for security at a hospital said that access to areas within a facility will also probably remain more tightly controlled.

“We’ve gotten to the point where we’ve locked a lot of places down and that may stay because people have realized that it maybe isn’t that bad,” he said. “It’s not that time consuming to check to see who’s coming in. It’s not that time consuming to say, ‘Are you supposed to be here?’ [Hospital personnel] have seen that it can work. In the past, if you tried to lock something, you would get pushback: 'What about my patients?' But now they've seen that it can work, and it's not that difficult, so I think a lot of people are going to like it, and I think a lot of it is going to stay in place."

In terms of identification for access control, the deployment of touchless, frictionless systems, often leveraging biometrics, offered a way to support pandemic efforts to maintain social distancing and minimize contact with surfaces. Even under more normal conditions, those technologies will stay in use and could expand.

"There are different technologies that are starting to come out there, and we're exploring all those options, [including] touchless … ticket scanning," the emergency management director for a university with one of the nation's largest college football stadiums said. "Our screening that we're looking at for [fall 2022] will be the same way. It will be pretty much walking through a magnetometer. You shouldn't have to touch anybody to pat them down or anything."

On the surveillance and situational awareness side, the ability to observe locations remotely, often through a security-as-a-service (SaaS) model, was found to offer significant value during both a pandemic and regular operations.

"Secured remote access to security networks allowed professionals to monitor, maintain and operate [security operations centers] from the house," a real estate security director said. "This trend will continue as cloud-based systems evolve. Although probably standard for larger corporations and similar to a vSOC for cybersecurity, remote SOCs will likely become a true secondary command option versus a physical location for many companies and organizations. Maybe even primary for some."

Finally, the reliance on cloud systems and remote monitoring, in addition to the growth in the number of employees who work from home, has underscored the need for robust cybersecurity, which has been a critical issue since long before COVID. And the victims of ransomware and other attacks have not just been corporations with deep pockets valuable information. Even public institutions like hospitals and schools have become targets of opportunity.

"The culture in K-12 just doesn't recognize the security value proposition," an IT director for public schools in a large U.S. city said. "We're still trying to make the case that security is important. As a result, many organizations are not very mature in their approach to security and the attackers know that…The FBI has put out multiple warnings highlighting the dangers to schools, and the big reason is the same that cybercrime occurs everywhere – its asymmetry. The attacker has the advantage in that relatively little effort can generate massive reward…We have a really steep hill to climb [to fund adequate cybersecurity] and that only makes us more of a target."

Finally, the reliance on cloud systems and remote monitoring, in addition to the growth in the number of employees who work from home, has underscored the need for robust cybersecurity, which has been a critical issue since long before COVID.

Conclusion

Security responses to the pandemic demonstrated how technology can enhance resilience and provide options when normal operations are difficult or impossible, while having the flexibility to serve additional – unplanned – purposes, such as virus mitigation.

Since 2019, SIA's Megatrends publication, which identifies the top 10 security technology trends identified by industry leaders, has had cybersecurity at either No. 1 or No. 2. Each of the past three lists has also included the cloud, SaaS models, and artificial intelligence, which has an important role in video analytics, all of which had unique value during the pandemic.

The cloud, in addition to being a trend on its own, is a part of each of the other named trends, and a poll commissioned by a European security solutions provider in early 2021 found that "78% of the 1,000 senior decision makers surveyed anticipate their organizations' use of cloud technologies to increase in the future as a result of COVID-19."

The combination of these factors, meanwhile, adds up to a broader trend. When Megatrends was released in 2019 and 2020, this was generally identified as the Internet of Things. Last year, however, "Security as Proptech" – which, generally speaking, involves leveraging various IoT, smart building and other technologies to optimize real estate, especially residential, sites – effectively took its place. Memoori, a Sweden-based research firm that focuses on the smart building industry, noted in January 2022 that, "Over the past two years, as the COVID-19 pandemic challenged all industries, we have seen physical security thrive in many aspects of this new environment, driven by virus mitigation and the convergence of physical security with the…IoT in smart buildings."

The pandemic's lasting impact on security, then, appears likely to be an acceleration of multiple trends using technology as force multipliers that were already underway.

78%

Of the 1,000 senior decision makers surveyed anticipate their organizations' use of cloud technologies to increase in the future as a result of COVID-19.

SIA
SECURITY INDUSTRY ASSOCIATION

securityindustry.org

SECURITY INDUSTRY ASSOCIATION

securityindustry.org

Sponsored By

maize marketing