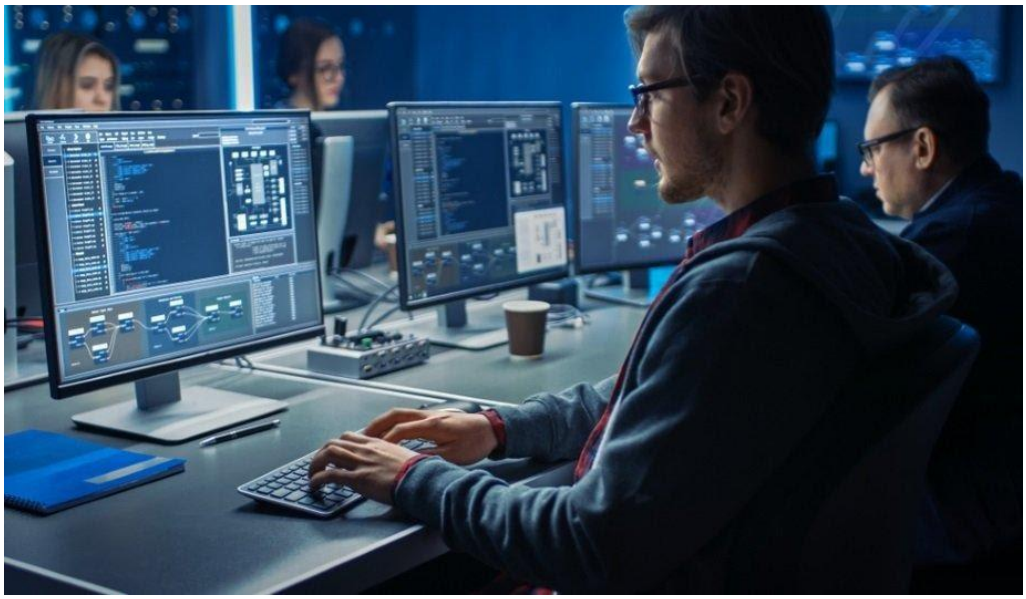
securityinformed.com
Making The World A Safer Place

What Will Be The Biggest Surprise For Security In 2023



Larry Anderson

23 Dec 2022

Like any year, 2022 was full of surprises for the physical security industry. Adapting to supply chain shortages, lightning-fast technology development, and changing occupancy patterns in a shifting labor market were just a few

of the factors that kept security professionals guessing in 2022. Wonder what the new year will hold? We asked this week's Expert Panel Roundtable: **What will be the biggest surprise for security in the year ahead (2023)?**

David Smith Identity One

The COVID-19 pandemic has changed our understanding of contagious diseases. From reducing physical contact to maintaining distance from others, many COVID-era norms are here to stay. For the physical access control industry, this means limiting physical contact with equipment, card readers and door handles will continue to be important—in 2023 and beyond. It is no surprise 'touchless' technologies thrived throughout quarantine. However, it may surprise industry professionals how important these tools will remain, going forward. In 2023, the responsibility will fall on organizations to enable individuals to enter a secure area without the need to touch any surface or carry any badge, token, or cell phone, ensuring employees and visitor safety without compromising security. Many touchless technologies exist today, such as facial recognition, fingerprint readers and voice pattern recognition. Which emerges as the most cost effective and least intrusive, however, will win the day.

Fred Burton Ontic Technologies

In 2023, growing social and political polarisation will limit the number of resources to effectively prevent and investigate crime. Organizations with publicly accessible storefronts face the most significant problems, since in many cases, the security measures necessary to meet compliance

requirements and ensure the safety of personnel and assets may exceed profits. Furthermore, maintaining a visible security presence may increase the potential for violence, rather than diminishing the threat. In the year ahead, organizations will likely be surprised by the lack of resources and ultimately will need to be prepared to fill the gap. Organizations will begin to pay higher prices for trained and qualified protection professionals, while also shifting their paradigm to address threats using protective intelligence. Overall, filling the void and preventing threats will require that security teams and companies hire protective intelligence analysts and invest in technology and early warning data that allows security teams to be proactive.

Sheryl Pinckney-Maas **Guardian Zone, LLC**

November 5th marked the one-year anniversary of the fatal 2021 Astroworld Festival (in Houston, Texas), which left ten dead, 25 people hospitalized and many more with minor injuries. Though incidents like crowd surges, medical emergencies, and egregious behavior (e.g., fights, theft, sexual assault, and active shooters) happen regularly at large venues, this event has remained top-of-mind in the live music industry. In many ways, it reminds us how little control we have during such incidents. Now that large event attendance has returned to pre-COVID numbers, I expect the biggest surprise for the security industry will be that event security staff will be overwhelmed during these kinds of incidents. Not many fan engagement security improvements have happened since Astroworld. As attendance numbers continue to grow, it will become imperative to lean on cloud-based apps to provide

crowdsourced intelligence to improve incident response times and offer security personnel a force-multiplying tool.

Ken Poole Johnson Controls, Inc.

It may not seem surprising, but the way that technologies will continue to build off each other and work together will be important in 2023 and have a big impact on security, especially for IT, OT and cybersecurity as they continue to come together. These sectors have their clear links, and convergence in physical security trends will continue to gain traction in the upcoming years. Modern technology continues to blur the lines between the physical and digital worlds, and synergies between these sectors will deliver seamless and cost-effective solutions. Digital integration is also allowing for two-way communication between building managers and security professionals, giving them the opportunity to choose how they want to respond depending on the situation. Not only does two-way communication further the digital journey of security, but it also allows facilities to respond to each specific scenario in the appropriate and unique way that situation may require.

Brad McMullen 3xLOGIC, Inc.

One of the major changes I expect in 2023 is the return to the office — at least in a hybrid manner — for many employees who have been working remotely since the onset of the pandemic. This major shift back to employees being in physical buildings will drive companies to look for ways to utilize their existing security infrastructure to provide “beyond security” insights such as building occupancy, utilization, and management. We will

better understand the use of buildings via access control data including varying occupancy levels, times that people are transiting entrances and exits, movement within the estate, and more. This expanded role of electronic access control will provide additional opportunities for ROI from these types of deployments. Remote access control can allow the hybrid work approach to be as effective as in person. Security Administrators can add or remove credentials remotely for visitors or new employees. Video Management Systems can be used not only to perform security operations, but also for remote management of people access to secure spaces, verification of access requests, interactive hosting, and improved business insights.

John Davies TDSi

They aren't perhaps that surprising, but two trends that I think will dominate the security scene in the year ahead will be increased cyber threats and the broader adoption of AI in more market segments. Cyber threats are always a concern, but current global instability amplifies this further. A new survey from IEEE that polled 350 senior IT people, showed that 51% of respondents mentioned cloud vulnerability as a top concern (up from 35% in 2022) and 43% mentioned data center vulnerability as a top concern (up from 27% in 2022). Other areas of concern include ransomware attacks (30%), coordinated attacks on an organization's network (30%), as well as a broader lack of investment in security solutions (26%). With physical security systems being a key part of the IoT mix, the cyber security element cannot be underestimated. Also, as many sectors look to do "more with less," the use of some elements in the AI "kit bag" will see it being introduced in more market segments. A prime focus might be in the areas of building automated

security systems, natural language processing, face detection, and automatic threat detection.

Kayne McGladrey Hyperproof

One of the biggest surprises for 2023 will be how many boards of public companies are suddenly recruiting for board members with cybersecurity expertise. Under a draft rule proposed in 2022 by the SEC, companies will need to disclose who on the board is responsible for cyber risks, how often they're informed about cyber risks, and their relative cybersecurity expertise. We're already operating in a world with a high degree of media attention to breaches and a persistently high level of job openings in cybersecurity. In a recent IEEE survey of global technologists, 51% of respondents mentioned cloud vulnerability as a top concern moving into 2023 (up from 35% in 2022). Boards will need to decide how to manage the very real risk of reputational damage and related risk of loss of institutional investor confidence due to mandatory SEC disclosures that show if a given company has no one with a background in cybersecurity risk management.

Eddie Reynolds Iluminar

We learned a lot of important lessons during the COVID-19 pandemic. If 2020-2022 were years of reflection and reorientation, I expect 2023 to be a year of extensive rebuilding. In the long run, I think the businesses that will thrive will be those who join the collective push to diversify its workforce to include women and minorities. Of course, this is no small task. And the work required will extend far beyond 2023. But in my opinion, it is imperative that the industry commits itself to changing with the times. I look forward to

seeing more companies and industry organizations empower and recognize women and minorities in positions of influence.

Fredrik Nilsson Axis Communications

Video analytics technology, often referred to as AI, will continue to accelerate. AI has been quietly used to automate certain security and business processes for some time now, but the use will become more widespread, and we are going to see new and exciting use cases emerge in the coming years. AI is already a part of your security stack whether you realize it or not – and it will soon enable even more advanced analytics based on video, audio, and other data. These analytics will provide important security insights as they always have, but they'll also generate valuable new business and operational intelligence. We're on the verge of the AI tipping point, and organizations who invest in video analytics are in a ripe position to flourish in 2023.