Insights on the Paradigm Shift in Video Surveillance Technology

End-users have partnered with integrators and vendors for a new approach to business operations

by Steve Lasky

Courtesy of BigStock.com -- Copyright: kentoh

Already regarded as the most dynamic and volatile security technology market, the trajectory of video surveillance systems has dramatically transformed these past 15 months due to COVID-19. The coronavirus pandemic accelerated the adaptive process of advanced analytics and AI integration into video devices to help governments, organizations and business owners track and help mitigate the spread of the deadly illness. From integrating video with secured entrances and physical access control to monitoring temperatures and tracking people throughout a facility, video systems have been instrumental in both curbing further outbreaks but also helping to restore quasi-normal business operations for many organizations.

As market sectors across the country continue to strategically reopen operations, video surveillance figures to remain in the spotlight. Recently Editorial Director Steve Lasky conducted a virtual roundtable with representatives from Hanwha Techwin, their affiliates and clients to better understand the ramifications of COVID-19 on the perception of security video technology in the recovery and what the future has in store. Joining me are Ray Cooke, Senior Vice President for Products, Solutions, and Integrations at Hanwha Techwin America; Don Fruhwirth who is the Director of Product Management at Interface Security Systems; and Lee Brown, who has worked 19 years in a lead role for the design and operation of casino video surveillance systems.

Steve Lasky: *How has the pandemic forever altered the realities and perceptions of what video surveillance technology is meant to do and should do?*

Ray Cooke: As a manufacturer serving our customers around the world, we've seen just how important

video surveillance has become to businesses operating with reduced staff and a remote workforce. The pandemic has been a proof point in how video surveillance technology can be expected to go beyond traditional physical security in providing new ways to protect customers, employees and assets. Beyond capturing images, the ability for cameras to collect and analyze data has increased their utility in ways that positively impact sales and operational efficiency. The way in which analytics and AI could be deployed at the edge during the pandemic is a testament to the agility and development speed that is possible when a market or public safety need arises. Being able to update and enhance a camera that someone has already purchased is a powerful way to add value and represents a departure from old business models. Post pandemic, this same AI-based, license-free analytics that monitored occupancy levels and social distancing will evolve to monitor traffic congestion and provide actionable retail intelligence.

Don Fruhwirth: This crisis has given the security industry an opportunity to redefine its role and value proposition. Security technology is no longer seen as devices that are solely used to keep people and property safe, but it is finally becoming a strategic tool to help improve business operations. AI-based security solutions and cameras are now able to go beyond security to capture valuable marketing and sales transaction data, analyzing customer patterns and behavior. By leveraging business and operational intelligence data that can pay for itself and directly affect the profitability of the organization, the security industry is on the cusp of morphing from a tactical application to a truly strategic enterprise-shaping role. As long as a privacy-by-design approach is taken, there is no reason to slow innovation or the development of useful and exciting technologies like AI, face recognition, and others.

Lee Brown: The pandemic showed us how important it was for all facets of our technology to be adaptable in an organization. As technology matures, better designs typically find greater market acceptance. Aside from a product's reliability, the degree of value we place on a design is a direct reflection of the product's current utility. Beyond fulfilling its basic intended use case, technology needs to be interoperable with open or industry-accepted standards.

A surveillance camera or VMS should be easily controllable and configurable to provide maximum value to the end-user. Many organizations found themselves having to do more with fewer resources during the pandemic. Adaptability and flexibility are the order of the day when it comes to what new video surveillance technology should do. New video surveillance technology should also interoperate with other data-driven technologies across on-premises, hybrid and cloud-based infrastructures.

» The pandemic has been a proof point in how video surveillance technology can be expected to go beyond traditional physical security in providing new ways to protect customers, employees and assets «

Ray Cooke, Senior Vice President for Products, Solutions, and Integrations at Hanwha Techwin America.

Lasky: *COVID has created a paradigm shift in the discussions of security on-premises and cloud-based surveillance architectures, which will have a significant impact on the industry in the years to come. How do video surveillance technology and applications fit into this roadmap?*

Cooke: It's important to separate the concept of cloud video storage from using the cloud to manage infrastructure and security systems from a distance. For most users, a hybrid approach will be the way forward with regards to storing video. The cloud represents an expensive place to store video streams with nothing going on in them. It can be a great place to collaborate and share footage of a particular event with a loss prevention team. We are keenly interested in supporting a balance of on-prem advantages with those of the cloud for video management, and thus we support a robust ecosystem of cloud video management solutions. Using the cloud to securely manage connections between remote, mobile and on-premises VMS and storage systems is an example of how our WAVE Sync application lets people interact with their security system every day. And when it comes to support, you want to avoid rolling a truck to check on a camera or do maintenance. Cloud management also gives integrators the tools to diagnose and triage faults and issues remotely which further reduces the TCO of a system.

Fruhwirth: During the pandemic, the security industry got a significant wake-up call to accelerate its digital transformation. In order to not just survive but thrive, our industry will have to let go of the false division between

cloud and on-prem and embrace hybrid deployment models. By doing away with this dichotomy, security leaders can make decisions about how they want to bring scale, redundancy, and availability to their business in a way that suits their deployment and ownership needs. Leading organizations will look beyond devices and sensors to technology that can encompass the entirety of the security operations workflows and how it can facilitate deeper operational and business insights as well as build a stronger posture towards compliance and cybersecurity. A chain is no stronger than its weakest link. Hence, it is critical to work with a security integrator that can demonstrate deep cloud, cybersecurity and network design expertise to eliminate those weak links.

» During the pandemic, the security industry got a significant wake-up call to accelerate its digital transformation. «

Don Fruhwirth is the Director of Product Management at Interface Security Systems.

Brown: COVID has already had a profound effect on design review and elicited greater contemplation from developers and designers. The same analytics algorithm that detected faces in an image pre-COVID can now be used for mask-wearing compliance. For manufacturers like Hanwha, this was a simple modification or update that offered stream-lined delivery to new and existing customers. On the other hand, developers saddled with poor, cumbersome, or inflexibly designed products found that implementing these kinds of changes proved very costly. Cloud-based storage infrastructure may not be for everyone. Cloud-based management certainly makes the most sense for collaboration and remote workflows. Whether it's for a cloud or on-premises solution, any development roadmap must be well contemplated in terms of the fit for the customer. If it's not, I think there are consequences for the brand in the way that customers will view the product.

Lasky: *As we move forward from the pandemic, the landscape of security has been changed forever. Do you see expanded roles for video surveillance in our future-proofed world?*

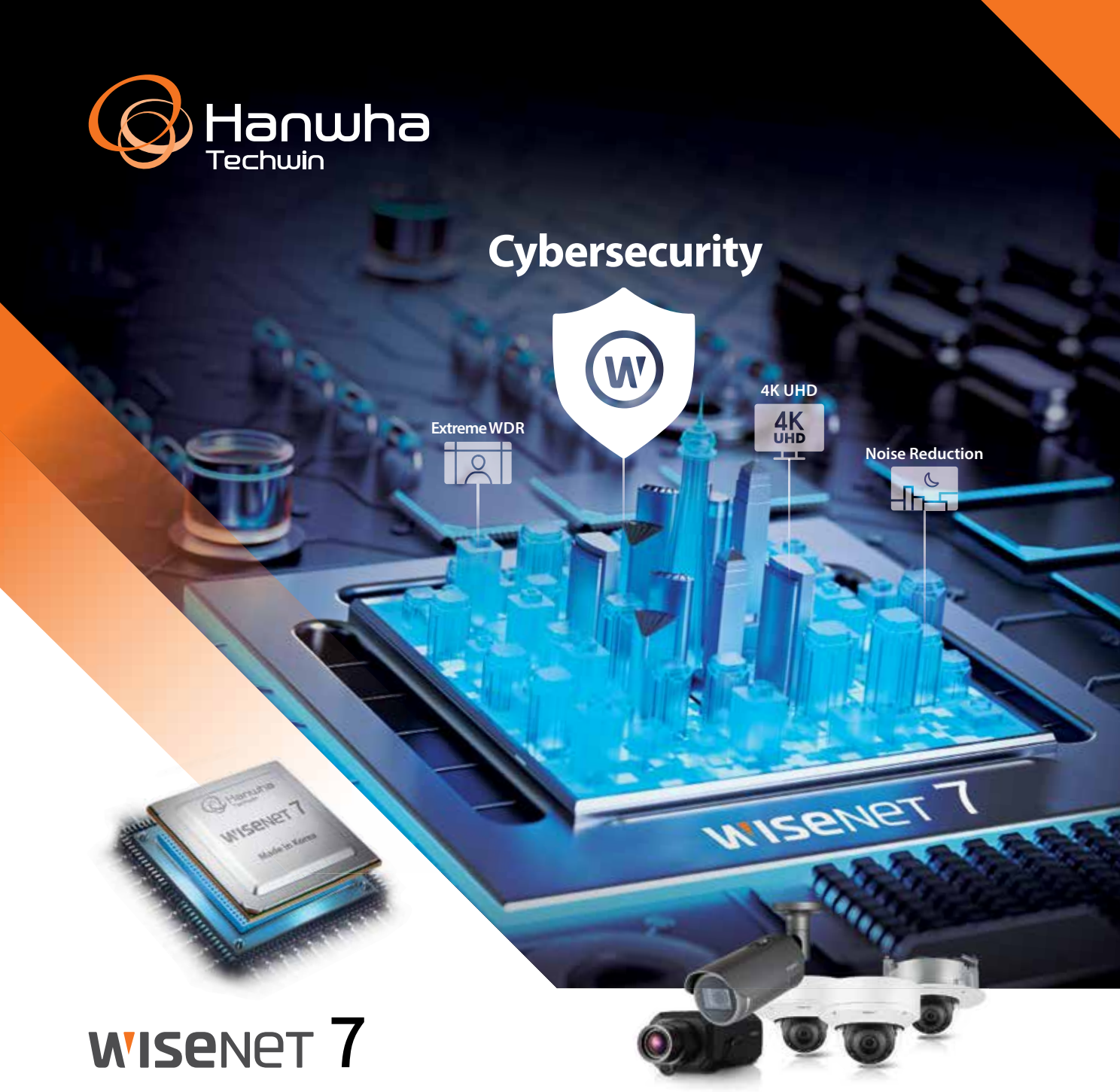
Cooke: The security industry really had to step up during the pandemic. Threats were ever-present with empty buildings and fewer employees, and fresh vulnerabilities were exposed as people scrambled to work remotely. The value of having a comprehensive surveillance system in place was repeatedly demonstrated. At the same time, many organizations quickly discovered weaknesses that need to be addressed in regard to false alarms and having insufficient resources to validate potential threats. In order to be future-proofed, security systems need to be more proactive in their ability to help us know when an event needs our attention. Traditional motion-based analytics aren't reliable enough which is why AI-based analytics will be a key part of any proactive solution. Object detection and descriptive metadata all but removes false alarms and give operators the information they need to make timely, informed decisions in real-time while drastically reducing the time required for post-event forensic search. It's time to start using cameras more and more as the versatile, practical IoT sensors that they are now meant to be. Once we start to think differently, then a world of possibility opens up for how we use this data to improve customer experiences, streamline operations and increase revenue.

Fruhwirth: Absolutely. As businesses gradually return to pre-pandemic staffing levels and hours of operation, a lack of available resources will continue to be a challenge for many. Security systems can play a major role by providing more eyes and ears on the ground. By utilizing AI-based analytics, staff can be alerted in real-time to important events that need their attention. Video verified alarm services that integrate video surveillance and alarm systems together can reduce false alarms and avoid nuisance calls and fees. For lone workers or minimal staffing, a virtual guard service can watch over the premises and announce its presence with voice-down notifications from a professional monitoring service. In addition, personal protection devices can be integrated with video surveillance solutions to protect lone and mobile workers. AI-based analytics can also provide insightful data for sales and marketing teams to identify peak periods and monitor customer flow and interaction throughout a store. All of these technologies and services can help workers feel more secure while simultaneously providing a solid path to profitability.

Brown: I do see expanding roles for video surveillance that move beyond the "one size fits all approach" to application development and delivery. Well-conceived tools will need to be made available to the end-user and/or integrator. The tools will need to empower the customer to author classifiers, and other machine learning (ML) / neural net (NN) type solutions that can be built locally, embedded in edge devices, or coupled

Hanwha Techwin

Cybersecurity



WISENET 7

End-to-end cybersecurity

Hanwha Techwin's commitment to cybersecurity begins at the factory, and never stops.

We embed unique certificates and encryption keys into every product. We make, assemble, design and fabricate our own chipsets and components, forming a "Supply Chain of Trust." Our new UL CAP Certified cameras with the Wisenet 7 SoC meet the industry's most rigorous cybersecurity evaluation criteria.

The result: a fully secure, end-to-end surveillance workflow you can trust.

HanwhaSecurity.com

Request information: www.SecurityInfoWatch.com/10215711

with the VMS either on-premise or in the cloud.

These customer-authored solutions might also be shared or modified by other users in some type of vetted ecosystem or repository. Excepting the NN and ML components, we are witnessing an explosion of activity around home automation applications and devices.

Applications like Home-Assistant and Node-Red offer the customer a way to integrate widely disparate devices/apps in a convergent or best fit solution whether on-premise or in the cloud. In contrast, services like Zapier and IFTTT may need to allow more localized control of devices and lessen rigid cloud-based dependencies. The video surveillance industry will likely witness an increasingly dramatic ebb & flow of demand between locally hosted and dependent cloud-dependent solutions.

» Data security must be strongly present during the inception of an application's development and persist or improve with each release cycle. «

Lee Brown has 19 years of experience in casino video surveillance design and operations.

Lasky: *With expanding privacy mandates across the globe brought about by GDPR, CPP and now the new Virginia privacy laws, how will video surveillance solution providers and end-users of the technology have to adapt to ensure that important forensic and information data is securely stored and encrypted to mitigate potentially devastating information breaches?*

Cooke: Robust cybersecurity is the first line of defense and although requirements can vary, more and more customers are demanding NDAA compliance and certifications like UL-CAP when it comes to devices running on their network. Making sure that only authorized people have access to the information goes without saying, but we also want their access to that information to be accountable. I think of this as "who's watching the watchers?" Having an audit trail when accessing video clips leads to more responsible and ethical use of surveillance technology. It's also become more important to understand and find a trusted supply chain — where did the parts and components come from in a device and where were they assembled and programmed? While our Wisenet 7 SoC is by far the most cybersecure product we have ever made, cybersecurity must constantly evolve to stay relevant. It's important for integrators and end-users to stay current with regular updates and improvements. Making that easy to do is a big part of proper system design.

Fruhwirth: It's crucial that any security installation addresses privacy as a core part of the design. As cameras become increasingly more powerful and feature-rich, their ability to capture personal identifying information (PII) continues to grow. Every organization needs to ensure that PII is handled in accordance with local laws and that any security system deployed is flexible enough to adapt and evolve as laws and best practices will almost certainly change over time. Privacy-by-design is the approach any manufacturer or integrator must take, where privacy features and functionality are built into the core design from inception and not simply an afterthought. These features should enable end-users to easily conform to best practices and mandates. Employees should be able to opt-in for touchless access, cameras should be able to mask out off-limit areas, and operator rights and privileges should ensure that only people who are authorized have access.

Brown: When data security is added to an application rather than being a design priority and intrinsic to the functionality of the application then it will likely fail to provide the desired level of security. Data security must be strongly present during the inception of an application's development and persist or improve with each release cycle. Simply fulfilling a compliance checklist is grossly inadequate. Attackers are under no obligation to constrain their methods. It is beyond obvious that a successful attack, even if technically minor, can impart incalculable damage to a brand. Monitoring, pen-testing, fixing and patching vulnerabilities are, in aggregate, far less costly than repairing a damaged trust relationship with customers.

Privacy mandates that relate to video storage all seem to trend toward encrypted storage, while some may specify that encoding or transmission must also utilize encryption. One of the less obvious elements noted in the GDPR relates to data accessibility. A patron might request a copy or deletion of content that contains their image or other identifying information.

Locating this content could impose a considerable burden absent the tools or recording infrastructure necessary to efficiently query for the requested data. Manufacturers need to take a 'privacy by design' approach that anticipates the need to adhere to evolving privacy standards.

SIA
SECURITY INDUSTRY ASSOCIATION

Vertical Insights Symposiums

K-12 School Security

July 29, 1:00 – 4:00 p.m. EDT

Register Online: securityindustry.org/k12security

An Interactive, Virtual Summit For School Security Leaders and Security Technology Professionals

- New school security risks
- Applying the latest technologies
- How to find project funding
- Meeting current guidelines

What to Expect

- Interactive, scenario-based training
- Virtual school security tours
- Practical sessions led by experts
- "Team Solve" participatory breakouts
- Real-time learning experiences

Sponsored by

ALLEGION™ DELL Technologies LENEL·S2 SALIENT

Produced With the Support of

SECURITY TECHNOLOGY EXECUTIVE · SIW SECURITY INFOWATCH.COM · SECURITY BUSINESS

Request information: www.SecurityInfoWatch.com/10215002

Security Industry Association
securityindustry.org

SIA SECURITY INDUSTRY ASSOCIATION