

A blurred, high-speed photograph of a crowd of people walking through a modern building's glass entrance. The image is dark and serves as a background for the report cover.

CAM 1

The Video Surveillance Report 2022

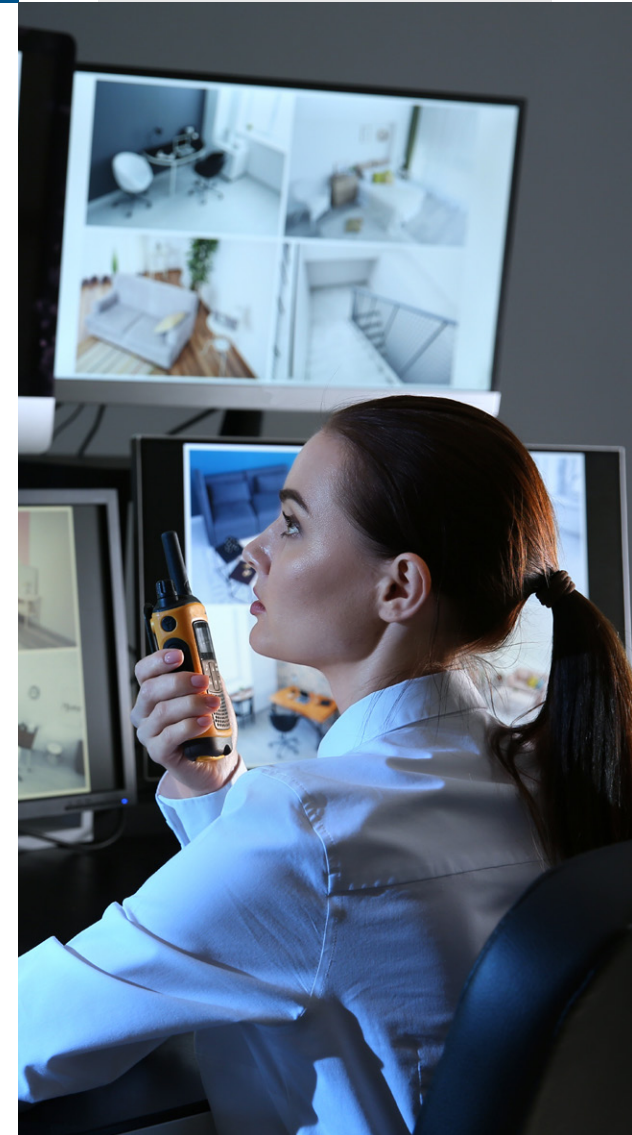
A trend report from

**IFSEC
GLOBAL**

01:22:11:00

Contents

Introduction	3
About the respondents	5
Demand for CCTV – Hardware & software	6
Cyber security and video surveillance	14
Vertical focus – Education, Healthcare, Logistics & Retail	18
Wider economic and geopolitical challenges: The impact on video surveillance	23



Introduction

Welcome to the 2022 IFSEC Global Video Surveillance Report, as we take our annual look at key aspects of the video surveillance industry to understand the current challenges faced by security professionals, as well as the future trends and opportunities.

While we would be hesitant to declare the pandemic 'over', this year is perhaps the first since 2019 where organisations and wider society may have felt a sense of 'normality' resuming – despite some regions continuing to be affected by the occasional lockdown.

Any sense of a return to market 'norms', however, was quickly halted. The invasion of Ukraine has created a new set of challenges to contend with, with the consequent impact on energy prices only just beginning to be felt by millions of people and thousands of businesses at the time of writing. Extreme weather events as a result of climate change have also continued to affect lives, while chipset shortages and supply chain disruption remain significant challenges for organisations globally.

No shortages of events this year, then. How though, are these wider geopolitical and socioeconomic factors impacting on demand for video surveillance projects? This is just one of the many facets we investigate in this year's Video Surveillance Report.

There is no denying that software in the form of video analytics or more sophisticated AI remains a central factor

behind investment in new video surveillance systems, and we'll continue to explore trends in this area with comparisons to last year's data. However, we'll also take a closer look at the hardware form factors most in demand and seek to understand the reasons behind the answers.

The report will also include a focus on cyber security – specifically in relation to video surveillance devices. Why? It's never been more in the public eye that any device connected to the internet carries an inherent risk of being hacked. Certainly, in the UK, national broadcasters have highlighted the realities of the challenge through dramatised programming – not just from lone actors seeking their individual fortune, but also from malicious and well-resourced nation states.

While video surveillance devices play a significant role in improving security, the fact that the majority are now networked also leaves them as potential targets to hack. So, where do professionals believe the vulnerabilities lie? And, most importantly, whose responsibility is it to 'protect the protectors'?

Finally, marking a change from previous year's reports, this year's survey attempted to drill down into a few specific verticals. Cameras are used across the globe by organisations in industries ranging from manufacturing to elite level sports clubs, but are there major differences in demand and trends for each?



Report written by
James Moore
Editor of IFSEC Global

To provide an answer to this, we explore four key verticals – education, healthcare, retail and logistics. Chosen based on the data available to us, as well as our understanding of popular growth areas for vendors in the sector, we asked those professionals who work directly, or have installed or consulted in the sector, to provide us with their views on the current demand for video surveillance projects the technology being used.

As ever, our thanks go to all those physical security, facilities and IT security professionals who have a role in specifying, installing or operating video surveillance systems who took the time to answer our survey. Without these responses, our reports are not possible to put together, so it is truly appreciated. We hope that the results outlined here provide the industry with useful insight to develop and inform their future business decisions – or at the very least, an interesting read!

And thank you to our sponsor, IDIS, whose experts provide additional insight into trends at various points throughout each chapter.

About the sponsor: IDIS

IDIS is the largest manufacturer of trusted South Korean-made video tech developed for a wide range of commercial and public sector markets.

Customers large and small choose IDIS video to meet their security, analytical and intelligence needs. End-to-end, NDAA-compliant solutions benefit from high performance, yet they are easy to install, operate and maintain and come with multi-layered, built-in cyber security. These combine to ensure a low total cost of service (TCS) for

NDAA
Compliant

Korean-Made
Video Tech That Users Can Trust



systems integrators, while end users benefit from extended warranties, forward and backward compatibility, and the flexibility to meet future requirements to deliver an industry-best low total cost of ownership (TCO).

Today IDIS operates across 50 countries supporting over 100 strategic partners with more than two million recorders installed worldwide, and over 16 million cameras utilising IDIS technology.

*Get the latest security news,
opinion and analysis delivered
straight to your inbox.*

*Sign up now for
IFSEC Global's weekly
security briefing.*



SUBSCRIBE



About the respondents

The survey was open to a range of roles in security, as well as those who manage, or are responsible for managing, buildings and facilities. IT and facilities professionals, whose influence continues to grow over IP-based surveillance device specification, were also included.

We asked end-users to specify the sector and size of their organisation to help ascertain whether there were any common themes in answers, dependent on industry. In addition, we removed certain job roles from the responses to particular questions, which were not directed at their role. By 'end-users', we are generally referring to in-house security, IT and facilities professionals, such as managers, directors or operators of surveillance equipment.

Anyone who selected 'not in the security/facilities profession' as a job role was automatically disqualified from the survey and has not been included in these results. We also received a number of attempted duplicate entries. We carefully assessed the final data to ensure that only those who we considered to be genuine responses from informed professionals are included in the results laid out in this report. In total, the 2022 Video Surveillance Report is based on the answers of 419 unique respondents.

Summary of respondents

The responses offer a global, overarching perspective of the video surveillance market, although a significant proportion came from the United Kingdom (38%). 15% came from

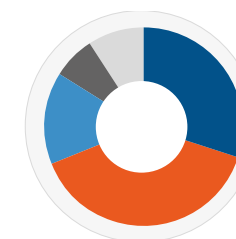
elsewhere in Europe, 8% from the United States, 7% from India, 6% from Nigeria, and 5% from South Africa, to cover the regions with the highest response rates.

Job roles varied within the industry. While many roles are now crossing over each other's responsibilities, there was a good distribution of roles that were represented. End-users made up 39% of the overall database, while installers/integrators followed at 30%.¹

Security or IT consultants provided 15% of responses, and 7% came from elsewhere in the supply chain, such as software vendors, manufacturers or distributors. The remaining 9% selected 'other', with roles covering security officers, site health, safety & security managers, estates managers, technical managers, law enforcement and building project management professionals.

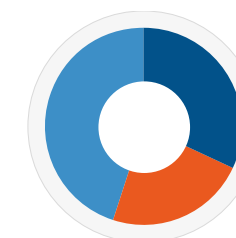
Key verticals from the end-user segments included manufacturing/engineering (13%), IT/cyber security (13%), education (12%), government (12%), construction (9%), and distribution/logistics (6%), though several in the 'other' category noted that their roles cover a variety of sectors. Transportation, retail, healthcare, finance & banking, hospitality & leisure, utilities, and residential housing were all represented, as well.

The size of end-user organisations varied – 45% work in larger businesses with over 250 employees, 23% in medium-sized businesses of between 51-250 employees, and the remaining 32% in small enterprises of 50 employees or fewer.



Job roles of respondents

- (30%) Installers/integrators
- (39%) End-users
- (15%) Consultants
- (7%) Distributors/vendors/other
- (9%) Other



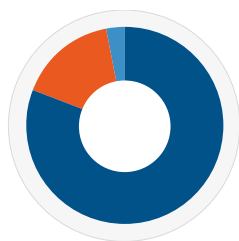
What size is your organisation? (End-users only)

- (32%) Small (50 employees or below)
- (23%) Medium (51-250 employees)
- (45%) Large (more than 250 employees)

¹ It should be noted that we have included 'Business owner/senior executive' in the end-user category for the purposes of this report, though we are aware that this may include some installers or integrators who run their own businesses.

Hardware, software and features – What do users want from today's video surveillance systems?

We found in last year's survey that today's video surveillance devices are used for so much more than just security purposes. Almost half of respondents in the 2021 Video Surveillance Report answered 'yes' when asked if their video surveillance was being used for operations outside of security² We investigated this a little further this year, finding that only 16% of those who are using AI or video analytics are doing so purely for security purposes.



Have you witnessed an increase in demand for new video surveillance projects/installs in the past 12 months?

- (81%) Yes
- (16%) No
- (3%) Demand has decreased

This data mirrors the British Security Industry Association's own recent 'Bigger Picture' report, which also found that 30% of CCTV deployments in the UK are being utilised for more than just crime prevention purposes.³ While there are some differences here, the BSIA data includes public and private sector use, whereas our own survey is primarily focused on those in private organisations.

We'll delve into exactly what video surveillance is being used for a little later, but there is clearly a requirement for newer video systems that can provide organisations with more tangible returns on investment than ever before. And, with 81% of systems installers answering that they have witnessed an increase in demand for new video surveillance projects in the past 12 months, this is good news for the market as a whole. What exactly are systems operators and end-users looking for, though?

Brand loyalty – Variety is a necessity

We've continued to examine the software behind video surveillance cameras in-use this year, yet, there remains many additional features that are required from a video surveillance device that are worth exploring.

In recent years, the video surveillance vendor market has been dominated by acquisitions, mergers, and buyouts –

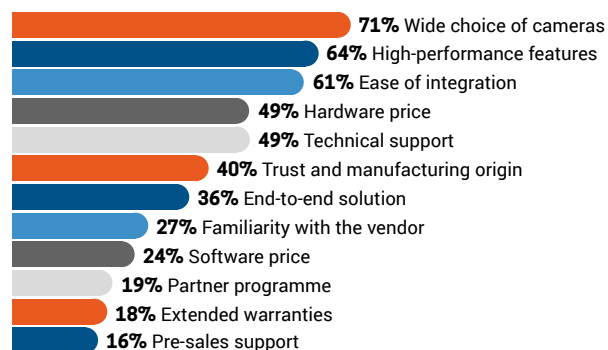


² IFSEC Global, The Video Surveillance Report 2021, <https://www.ifsecglobal.com/resources-1/the-video-surveillance-report-2021/>

³ IFSEC Global, BSIA's Bigger Picture report underlines growing use of video surveillance for business operational purposes, <https://www.ifsecglobal.com/video-surveillance/bsias-bigger-picture-report-underlines-growing-use-of-video-surveillance-for-business-operational-purposes/>

in the hardware space, at least. While new entrants have emerged, with some gaining significant ground – think the likes of 3xLogic, Arcules, Cisco Meraki, and Verkada – the majority of manufacturers of video surveillance hardware are well established brand names. Installers and integrators will tend to favour a particular vendor, or select few, as suppliers continuously innovate with new features, whether through their own research and development, or via third-party software integration partners.

What are your top reasons for choosing your preferred surveillance vendor(s)? (Installers only)



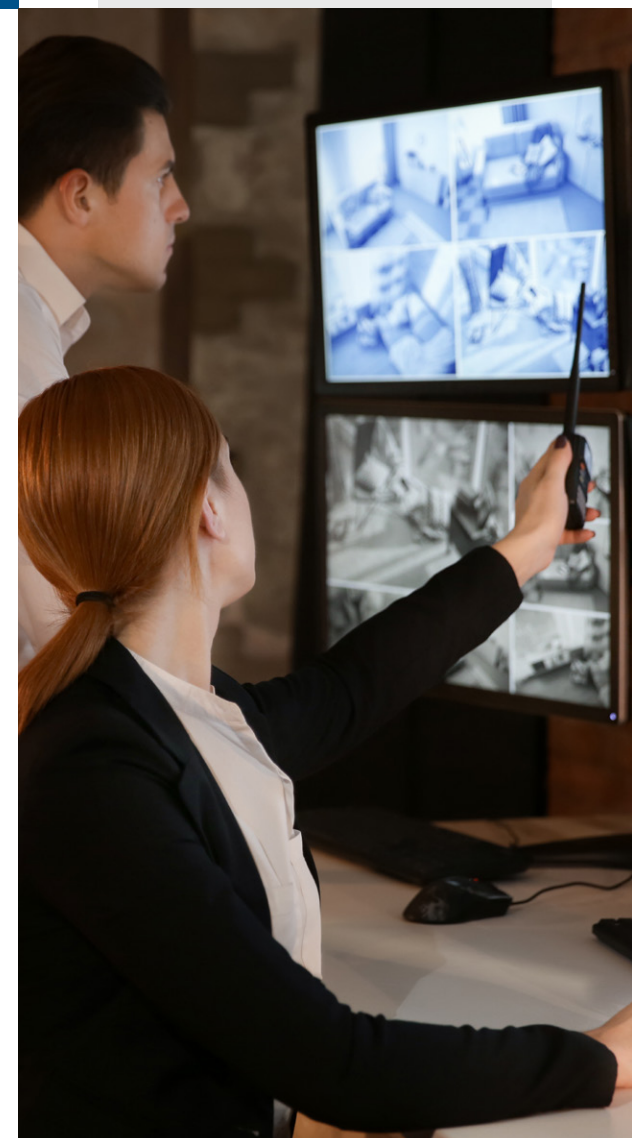
But what do installers of video surveillance systems value most when deciding upon which brand to use? It is of little surprise that a 'wide choice of cameras' (71%), and 'high performance features/functions' (64%) were classed as the first and second most important reasons for their choice. With so many options available, vendors must provide the full breadth in choice – from PTZ and analogue box cameras, through to 4K, AI-enabled options. The technology is readily available, so vendors may quickly fall behind if an installer can't provide the full suite of options to their customer from their preferred provider.

Also crucial is 'ease of integration'. 61% of respondents selected this as one of their top five choices, and it was a topic we examined in detail in last year's report, where 70% of those surveyed said they had witnessed increased demand for integration in 2021.⁴

James Min, Managing Director at IDIS Europe notes: "We're seeing increased demand for video integrated with access control and intruder systems, as organisations look to eliminate siloed systems that can cause gaps in security, and make operational efficiency gains. Looking ahead, customers will increasingly favour surveillance vendors that can demonstrate strong technology partnership eco-systems, giving them the assurance of long-term tech support, smooth interoperability, and a coordinated approach to cyber security."

While cost is regularly the biggest barrier to entry for upgrades and investment in new security solutions, it is interesting to note that it isn't always the most important factor in vendor choice. Hardware price was selected by just under half (49%) of respondents, and software price – an increasingly important factor for integrators and installers moving to a recurring revenue model – was chosen by 24%.

Just as important as hardware price was the technical support available from the manufacturer (49%), while 'trust and manufacturing origin' of the brand and 'familiarity with the vendor' were chosen by 40% and 27% of those surveyed respectively. Brand loyalty understandably plays an important role, it would appear. This isn't necessarily a surprising statistic, as familiarity allows engineers to quickly get up to speed with the installation process, and build up sound knowledge of the software and a particular vendor's offerings. Meanwhile, supplier relationships have



⁴ IFSEC Global, The Video Surveillance Report 2021, <https://www.ifsecglobal.com/resources-1/the-video-surveillance-report-2021/>

always played an important role in the security industry – distributors, local sales representatives and technical support teams are integral to building trust in a brand.

Whether the same level of loyalty will continue to flourish as the next generation of installers and engineers enters the market will remain to be seen. Open systems and standards are making it easier than ever to integrate video surveillance systems from disparate brands, while the physical installation of the cameras themselves has changed significantly with wireless IP devices that connect to the cloud. Wiring and setting up on-premise DVRs and NVRs are not necessarily a requirement, while manufacturers continue to make it easier than ever to install their devices and build in plug-and-play functionality.

“Even smaller organisations are looking beyond the upfront price of hardware. After years of ripping-and-replacing cheap hardware that delivered poor performance or resulted in high maintenance burdens, businesses are evaluating lifecycle costs before making purchasing decisions. Every project is different, but in many cases, we are seeing NDAA-compliance becoming a more important factor, in Australia, Europe, and Southeast Asia as well as critical infrastructure projects in the Middle East. Fair and transparent ongoing licensing fees for VMS functionality and video analytics are also high on the agenda as business look to streamline OPEX costs,” adds James Min.

Partner programmes and extended warranties scored relatively low in the options given (at 19% and 18% respectively), indicating a level of market consistency, where vendors are likely offering similar schemes or offers across the board.

36% of respondents selected ‘end-to-end solution’ as one of their top five reasons for choosing their preferred video surveillance vendor. Available options in this sector are growing, with several case studies underlining this point, despite specific providers such as Milestone and Genetec remaining dominant market players at the end-point as CCTV manufacturers offer direct integration with one, or several, storage or VMS providers.⁵

Overall, all available options were considered relatively important – almost one in five were still selecting the least popular answers – underlining that several factors play a role when it comes to a preferred choice of video surveillance brand.



James Min
Managing Director, IDIS Europe

IDIS DirectIP® end-to-end surveillance that simply works

IDIS was the first vendor to offer true end-to-end video tech solutions that deliver guaranteed, seamless interoperability and inherent cybersecurity in a true plug-and-play solution. Today, DirectIP includes an extensive range of high-performance, NDAA-complaint cameras; recorders; accessories; and choice of scalable video management software and AI options that are all quick and easy to install. That means a lower cost of service (TCS) for systems integrators working with a one-stop-shop supplier, and on-time, on-budget projects. And end-users enjoy the IDIS promise of an unparalleled low total cost of ownership (TCO).



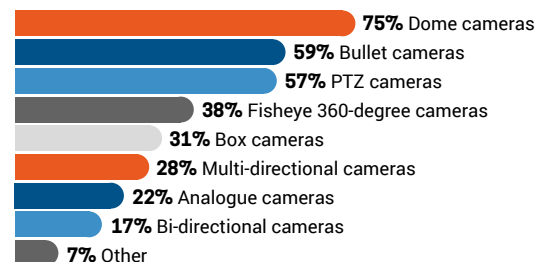
⁵ See as examples: End-to-end video solution utilised by Belgian DIY retailer, <https://www.ifsecglobal.com/video-surveillance/idis-end-to-end-video-solution-utilised-by-belgian-diy-retailer/>; London student accommodation security upgraded with end-to-end video surveillance system, <https://www.ifsecglobal.com/video-surveillance/london-student-accommodation-security-upgraded-with-end-to-end-video-surveillance-system/> or “...

Hardware form factors – dome, bullet and PTZs reign supreme

Variety is also important in the types of cameras that manufacturers are offering. We asked all respondents what types of surveillance camera devices they had installed in their organisations, or had been installing in the past 12 months. Dome cameras were deemed as the most popular, with 75% of respondents selecting this option, followed by bullet cameras (59%), PTZ cameras (57%) and fisheye 360-degree cameras (38%).

The proliferation of the internet and easy access to broadband, as well as technological advancements which have enabled prices of IP-based cameras to come down has resulted in widespread adoption of network cameras. Yet, one in five (22%) of respondents still identified analogue cameras as devices that they own, or that engineers have installed in the past 12 months. Clearly then, despite a lack of focus from vendor marketing campaigns and little coverage in industry press, analogue devices have a role to play and continue to be utilised.

What types of surveillance camera devices have you installed or had installed in the past 12 months?



"It can be difficult or expensive to replace coaxial cabling, and businesses often want to eliminate waste, and opt for a phased migration to IP without any downtime. This explains the continued demand for analogue surveillance. Using the latest IDIS encoders, customers can digitise a range of different analogue cameras' signals, mix-and-match with network cameras, and manage both from the same VMS. They can realise up to 5MP video quality if utilising HD-TVI. Modest yet steady sales, since the launch of the IDIS DirectCX line up of HD-TVI equipment over eight years ago, is evidence of the continued value of mix and match solutions," explains James Min.

Tech such as video analytics, AI, high resolution footage, wireless cloud storage and more has enabled the growth of IP devices over analogue in recent years. Not all situations call for such technology though, and if simple CCTV coverage for security and deterrent purposes is what's required, analogue devices remain a handy cost-effective option.

Surveillance tech – Do barriers remain for AI adoption?

Despite analogue still being in use, the adoption of modern cameras remains a clear trend. 42% of respondents have either adopted or installed edge-based AI cameras in the past 12 months, while 51% have either specified or installed, or are using deep learning powered analytics in their surveillance systems.⁶ Omdia analysts found that in their global control room market report for 2021, AI and machine learning are being applied to enhance control room offerings as the proliferation of AI chipsets continues in the video surveillance market, and our results match this insight.⁷



Continuing demand for the IDIS HD-TVI analogue range, particularly across Europe, says IDIS.

⁶ We should acknowledge that one of the answer options was slightly misworded in the survey for this question. The third option read 'no – we still implement/use traditional AI-powered analytics', which should not have included 'AI-powered'. This may suggest more than 51% of respondents would have answered that they were using AI in their surveillance systems.

⁷ IFSEC Global, Global control room market growing as AI and machine learning enhance solution offerings, <https://www.ifsecglobal.com/control-rooms/global-control-room-market-growing-ai-machine-learning-enhance-solutions/>

Barriers remain to adoption, of course. Of those who hadn't installed AI-based devices, 18% cited cost as the primary factor, while 31% said they were 'unsure of the benefits or definition of edge technology'.

What are the major barriers to implementing AI in surveillance systems?

Upfront costs	47%
Accuracy (false positive/negative alerts)	30%
Camera upgrade requirement	29%
Ongoing licence fees	24%
Storage concerns	11%
Upskilling employees	17%
Unsure of the benefit of ROI	23%
More trust in humans than machines	7%
Other	6%

We delved into the barriers of adoption a little more in a separate question. Upfront costs remained the primary barrier (47%), as well as upgrade requirements for their camera systems (29%) that comes with adoption and ongoing licence fees (24%), which have inevitable cost implications, too.

Despite continuous campaigns highlighting the potential benefits such tech can bring to an organisation, whether it be at trade shows such as IFSEC International, or traditional advertorials, there is a significant proportion of the industry that remains unconvinced of the genuine ROI (23%).

Reports of high false alarm rates won't help this situation, and this was reflected within the results, where almost a third of professionals cited accuracy as a barrier for adoption. For as many success stories the industry shares, there are inevitable challenges for others when implementing new technology. For instance, in a trial at an Australian care home, AI in the video surveillance system was found to have "neither negatively or positively influenced the quality and safety provided at the sites", with high numbers of false alerts.⁸

However, it was found that the AI improved over time as it 'learnt' and matured, with 22% of actual fall events detected by the CCTV technology, while several environmental factors played into challenges with the fall detection system. Despite lingering concerns, security professionals do at least trust machine technology, with only 7% citing they had more trust in humans as a barrier for implementation – compared to 15% in last year's survey.

Storage also wasn't as much of a concern as we've seen in previous reports. While surveillance systems with AI and deep learning algorithms require significant bandwidth and storage requirements due to high-resolution feedback, the proliferation of processing at the 'edge' of the network (on the camera itself), as well as the development of cloud storage solutions, is enabling greater accessibility to AI technology. This is reflected in the results – in 2021, 21% of respondents identified storage concerns as a barrier for adoption, whereas only 11% of respondents cited this reason this year.



⁸ IFSEC Global, AI video surveillance care home trial produced too many false alarms, say auditors, <https://www.ifsecglobal.com/video-surveillance/ai-video-surveillance-care-home-trial-produced-too-many-false-alarms-say-auditors/>

James Min comments: “Proliferation of AI is certainly bringing costs down, but we’re still seeing a lot of hype and overblown marketing claims, so it’s important to remember that human verification and intervention are still essential for control room operations. To guarantee minimal false alarms for the most important functions – including object, intrusion, loitering, and line cross detection, and facial recognition – you need a deep learning engine that has been developed over years using vast datasets.

“The IDIS Deep Learning Engine has been evolving and learning since 2017 and is proven to be 98% accurate. Giving credence to these results, it received Korean national certification in 2021 following testing for highly sensitive military and defence applications. It’s important not to overpromise, because not every application will lend itself to the very highest levels of accuracy, and users should look for certifications and evidence of testing in live environments. At the same time, we’re only at the beginning of the AI revolution, so as algorithms become smarter, we can expect a raft of new functions that will create safer and more secure environments.”

What’s in demand from camera features, AI and deep learning?

Just like the myriad types of camera form factors that are being fitted today, there is also a plethora of requirements of hardware and software features to suit the purposes of today’s surveillance systems.

From a hardware perspective, we asked what features will be required when purchasing their next camera – or if an installer, integrator or consultant, where do they see the most demand. High resolution or 4K cameras narrowly topped the list with 46%

of respondents – indicating an alignment with the push towards AI or edge-based systems that require better resolutions to work efficiently. If a camera can’t accurately identify a person’s face, facial recognition isn’t likely to work very well.

Durability appears to be an important requirement, too. 44% selected ‘IP66/water resistant cameras’, 43% ‘vandal resistant cameras’ and 24% covered cameras, all designed to protect from the elements or potential physical attack. Indeed, one in 10 said that ‘explosion proof cameras’ were in-demand – many of the end-users who selected these responses were from government, construction or manufacturing/engineering sectors.

Light enhancing cameras provide several benefits to operators, explaining why 40% of those surveyed said they were a feature that was in demand. Infrared capabilities above 30 metres was selected by a quarter of respondents, as was infrared capabilities under 30 metres, too.

Additional lighting on cameras can act as another crime deterrent, highlighting to potential intruders that clear footage is being recorded despite the surrounding darkness. Meanwhile, light enhancing capabilities can support analytics applications – not just providing clearer images, but also allowing thermographic and heat detection applications via infrared detection.

Moving on to the AI-powered software that’s most in demand, motion detection was cited as the chief driver for implementation by over half of respondents (59%). A useful tool in all applications, motion detection allows surveillance systems to alert camera operators only when necessary. Ideally, it would work hand-in-hand with object classification, whereby the system can recognise the difference between

What kind of hardware features will be required when purchasing your next camera? Or, if an installer/consultant, what features are most in demand?

4K/HD cameras	46%
IP66 rated/water resistant cameras	44%
Vandal resistant cameras	43%
Light enhancing cameras	40%
IR over 30 metres	25%
IR up to 30 metres	25%
Covered cameras	24%
True WDR	19%
Explosion proof cameras	11%
Heated cameras	10%
2MP or lower definition cameras	9%
Other	4%

humans (so genuine threats) and animals or inanimate objects that may have been blown through the line of sight by the wind, to ensure a reduction in false alarms. Object classification was cited by 41% of professionals, while reducing false alarms by 40%, underlining their importance.

Licence plate recognition systems (LPR) also appeared high on the list. One of the most commonly used features of AI for state departments such as the Police or Highways agencies to track suspects or spot parking violations, LPR is also growing in popularity for private organisations. Security professionals are able to match licence plates to people, providing an additional security measure for frictionless access control purposes to a private car park, for instance.

Viewed as a major differentiator between traditional video analytics and deep learning powered AI, 'critical event search' was identified by 42% of respondents for reasons behind adoption. 'People search' was also cited by another 23%. The ability to capture metadata, such as the colour of the clothing someone is wearing or the type of vehicle, allows operators to search through footage in a specified time window if an event were to occur.⁹ The AI is able to pull the relevant footage, potentially saving personnel from manually watching through hundreds of hours of footage, while simultaneously guarding against human error.

More traditional use-cases for video analytics purposes remain an important reason for AI adoption – proponents of AI highlight that such applications will be more accurate, while not requiring human intervention to adapt and teach systems, which the AI will do itself as it continually learns. Facial recognition was cited by 37% of respondents, people counting by 35%, loitering detection by 33%, customer behavioural analysis by 27%, and footfall analysis by 14%.

Top five reasons for video surveillance use outside of security purposes

1	Vehicle checks
2	Business intelligence
3	Workspace optimisation
4	Fire safety procedures/operations
5	General emergency preparedness



⁹ Chris Price for IFSEC Global, Is AI really necessary for video surveillance? <https://www.ifsecglobal.com/video-surveillance/is-ai-really-necessary-for-video-surveillance/>

An area that we've already touched upon – and one explored significantly in last year's report – is the idea that AI and analytics applications, and therefore the video surveillance systems they sit on, are no longer simply being used for security purposes. Further analysis is available from the 2021 report on this, but the trend has certainly continued this year.

Only taking into account those respondents who are using AI or video analytics, just 16% of them answered that they were 'purely using video surveillance for security purposes'. Vehicle checks remain the most common use by 43%, but business intelligence applications, such as those mentioned above – people counting, customer behavioural analysis, footfall analysis – are also popular use-cases (37%).

Meanwhile, 27% cited they were using them for workspace optimisation purposes. A particular growth area during the

pandemic, organisations that understand how their offices and facilities are being utilised can adapt accordingly – if one floor isn't being used, they can save rent, or if there are regular 'pinch points' in the warehouse, the layout could be altered to enhance efficiencies.

There is also the awareness that video surveillance can be used more holistically to help organisations prepare and predict for potential emergencies. 24% are using AI or analytics to enhance their fire safety procedures, while over one in five (22%) have spotted the potential to prepare for 'general emergencies' via video surveillance. Indeed, 11% are even using systems to predict and prepare for extreme weather events, such as to spot rising water levels or monitor localised environments that may impact a business from operating at full capacity.

Deep-learning powered solutions to suit businesses and budgets of any size

As an end-to-end video solution provider, IDIS offers a range of AI-powered analytics options to serve a variety of applications – from software-based deep learning and AI box appliances, through to edge AI cameras.

Developed over more than five years, IDIS Deep Learning Analytics (IDLA) delivers highly accurate line-cross detection, loitering detection, and object detection, all of which are much less prone to being triggered by harmless environmental factors than traditional analytics. Instead of continual attention being needed to focus on multiple camera streams, system operators only need to view a single video feed and decide on what action to take when a real event or threat occurs.

Customers can take advantage of 98% accurate IDLA module as a one-off payment within IDIS Solution Suite VMS without any ongoing license fees or device connection costs. And from late 2022, IDIS will start shipping a versatile range of 5MP AI cameras that feature its powerful deep-learning analytics on edge, with 8MP models due for launch in 2023.

IDIS Deep Learning Analytics (IDLA)

Powered by the
IDIS Deep Learning Engine



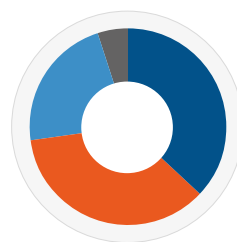
Member of KOREA

intel
partner
Gold
IoT
Solutions

Video surveillance and cyber security – Protecting the protectors

According to the UK Government Cyber Security Breaches Survey, 39% of businesses experienced a cyber-attack in 2021, at an average estimated cost of £4,200.¹⁰ In September of 2022 alone, there have been several high-profile cyber security breaches. Australia's second-largest telecommunications company, Optus, reported a significant data breach in September, ride-sharing service Uber was breached through a sole employee's network access, and a teenage hacker was able to infiltrate Rockstar Games' (the developer behind the Grand Theft Auto video game series) through an internal Slack communications channel.¹¹

That's not to mention the proliferation of state-sponsored cyber-attacks aimed at governments and critical infrastructure, either. The wider public is becoming more aware of the threat as data breaches make mainstream news outlets on a daily basis, while broadcasters have dedicated entire TV shows to cyber breaches. The BBC's *The Capture*, for instance, has highlighted the growing threat of deepfake technology, calling into question the reliability of CCTV and video surveillance footage – once thought to be a futuristic threat, now very much real.¹²



How concerned are you about the vulnerability of your surveillance system to cyber-attacks?

- (37%) Very concerned
- (36%) Quite concerned
- (22%) Not really concerned
- (5%) Not at all concerned

While the accessibility of highly sophisticated deepfake footage may not be quite the type of threat most organisations face, the need to ensure CCTV systems are protected from a cyber-attack is very much a genuine concern in 2022 for security, facilities and IT teams. As we've already discussed, most video surveillance systems now utilise IP-based devices, and therefore can be hacked.¹³

The majority are not missing this point. 73% of respondents answered that they were either 'quite concerned' or 'very concerned' about the vulnerability of their surveillance system to cyber-attacks.



¹⁰ Department for Digital, Culture, Media & Sport, Cyber Security Breaches Survey 2022, <https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2022/cyber-security-breaches-survey-2022>

¹¹ BBC News, Australia phones cyber-attack exposes personal data, <https://www.bbc.co.uk/news/technology-62996101>; Forbes, Social Engineering: How a teen hacker allegedly managed to breach both Uber and Rockstar Games, <https://www.forbes.com/sites/siladityaray/2022/09/20/social-engineering-how-a-teen-hacker-allegedly-managed-to-breach-both-uber-and-rockstar-games/?sh=2f208fec451c>

¹² BBC, The Capture, <https://www.bbc.co.uk/iplayer/episodes/m00085sx/the-capture>

¹³ IFSEC Global Podcast, Episode four: Converged security and the evolving role and risks of IoT, <https://www.ifsecglobal.com/podcasts/episode-four-converged-security-and-evolving-role-and-risks-iot/>

Where do the vulnerabilities lie and who is responsible?

From a video surveillance perspective, once a device has been subject to a successful cyber-attack, the entire network is then potentially at risk. While there is a benefit to hacking a camera itself, enabling footage to be tampered with or switched off for valuable seconds during a physical breach, the access to the overall organisational network is likely to be the end goal for many hackers.

There is little doubt then, that every device that is installed onto a system should have the adequate protections. Yet, professionals remain concerned across several areas. We asked what respondents thought is the single biggest vulnerability in their surveillance systems, and the risks appear to be relatively spread. Either this indicates that the industry as a whole is a little unsure of itself in this arena, or that there is a genuine concern that multiple factors are at fault for potential vulnerabilities.

Unsurprisingly, given most respondents were purchasers of video surveillance equipment rather than suppliers, manufacturers were deemed to be the ones most responsible for cyber-risks. A quarter of those surveyed said that 'back doors created by manufacturers' was the single biggest vulnerability in surveillance systems, while 30% confirmed that they thought manufacturers/vendors held the most responsibility for the cyber security of video surveillance systems.

Jamie Barnfield, Senior Sales Director, IDIS Europe, states: "It's disappointing that 'back doors' remain a priority concern since the 2020 report. Remote back doors cause gaps in cyber security that can be accidentally leaked or exploited by disgruntled employees and hackers. IDIS understood this risk as early as our brand launch in 2013.



What do professionals think is the single biggest vulnerability in their surveillance systems?

- **(25%)** Back doors created by manufacturers
- **(19%)** Negligent installation work/lack of education for installers
- **(14%)** Inadequate protections within surveillance hardware
- **(9%)** Inadequate education/support for end-users
- **(10%)** Inadequate internal organisational training/standards
- **(12%)** Inadequate protection elsewhere within the network
- **(11%)** Poor video management software design

"We also eliminated many cyber security risks that can inadvertently be caused by installers that don't have in-depth knowledge of routing or hole punching, by developing plug-and-play technology that mutually authenticates devices. IDIS FEN (For Every Network), is a one-click, automated network configuration approach that allows engineers to simply connect each site or branch store back to centralised control rooms. This streamlines cyber security and minimise complexity, and means that IDIS solutions have always been inherently cyber secure as well as faster and easier to install."

Lack of education is also a concern, it would appear. 19% were concerned that 'negligent installation work, or lack of education for installers' was the biggest contributor to vulnerabilities, 10% cited 'inadequate internal organisational training', and 9% 'inadequate education/support for end-users'.



Jamie Barnfield
Senior Sales Director, IDIS Europe

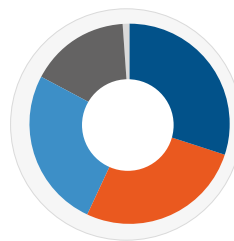
Many installers, integrators and systems designers will have traditionally focused on the installation-side of video surveillance equipment. There remains a huge demand for skilled engineers who can design and fit a series of networked (or cabled) surveillance devices which feed back into a storage solution. However, with so many of these systems now linked to the internet, whether it be on the camera itself, via cloud storage or through video management software (VMS), cyber vulnerabilities are increasingly common.

Who protects the protectors?

The argument between whose responsibility it is to protect systems continues to be a divisive one. Perhaps the most consistently agreed point is that it is everyone's responsibility – throughout the supply chain. From the very start, vendors should be building in cyber secure protocols, and protected methods of delivering continual software patches to protect from new vulnerabilities.

Building in cyber security from the start is something that the industry is now acutely aware of. The British Security Industry Association (BSIA), for instance, has launched a security equipment manufacturer's cybersecurity registration scheme through its special interest group, the Cybersecurity Product Assurance Group (CySPAG) only this year.¹⁴ Meanwhile, the IASME Consortium continues to encourage all vendors to be cyber vigilant and ensure their supply chains are cyber secure, via its Cyber Essentials scheme.¹⁵

Yet, as we can see from this year's results, security professionals understand the responsibility doesn't end with the manufacturers of physical security systems. Physical and cyber security have long been seen as separate sectors, but with the rise of smart buildings and the interdependence of physical systems with web-based networks, the boundaries between the two are becoming less visible. Systems installers must be aware of the cyber risk when connecting video surveillance systems to a network, with codes of practice now available to support in their roles.¹⁶



Who should be primarily responsible for the cyber security of video surveillance systems?

- (30%) Manufacturers/vendors
- (27%) Physical security end-users
- (26%) Cyber security/IT end-users
- (16%) Installers/integrators
- (1%) Consultants

¹⁴ IFSEC Global, BSIA unveils security equipment manufacturer's cybersecurity registration scheme, <https://www.ifsecglobal.com/cyber-security/bsia-unveils-security-equipment-manufacturers-cybersecurity-registration-scheme/>

¹⁵ IASME Consortium for IFSEC Global, Exploring the intersection of physical and cyber security, <https://www.ifsecglobal.com/physical-security/exploring-the-intersection-of-physical-and-cyber-security/>

¹⁶ IFSEC Global, New cyber security code of practice for installers unveiled by BSIA, <https://www.ifsecglobal.com/cyber-security/new-cyber-security-code-of-practice-for-installers-unveiled-by-bsia/>

Perhaps the biggest debate within this sphere relates to end-user responsibility – those operating and owning the video surveillance system. Traditionally very much under the physical security department's budget, the convergence between departments with IT and cyber security has never been clearer. Demonstrating the current nuances of the discussion, 27% of respondents believe that physical security end-users hold the most responsibility for the cyber security of video surveillance systems, while 26% said it was the responsibility of cyber or IT teams. Interestingly, there was no significant trend in job roles of those who selected these responses, indicating that there is no obvious answer to this question.

An electronic security system is often no longer an offline camera relaying footage through a cable. The integration of IoT and networked devices has meant that for any modern security solution, cyber and physical security can no longer be thought of as mutually exclusive and must work together to offer the best defence for an organisation.

Proponents of a converged strategy for end-users regularly argue that it is when these approaches are kept wholly separate, the risk of oversight and inefficiency is too great, resulting in an increased likelihood of security vulnerabilities.¹⁷ What is apparent, is the need for anyone manufacturing, installing, specifying or operating video surveillance equipment to remain cyber aware and vigilant, so as to ensure a security system doesn't cause the very opposite of its fundamental aim.



¹⁷ See Clive Madders for IFSEC Global, Why organisations can no longer ignore a joint approach to cyber and physical security, <https://www.ifsecglobal.com/cyber-security/why-organisations-can-no-longer-ignore-a-joint-approach-to-cyber-and-physical-security/>; Tom Kopecky for Dark Reading, Managing Increased Cyber-Physical Security Threats in a Hyper-Connected World, <https://www.darkreading.com/physical-security/managing-increased-cyber-physical-security-threats-in-a-hyper-connected-world>

Vertical focus – Education, Healthcare, Logistics & Retail

This year we opted to narrow down some of our survey research towards specific market segments. While video surveillance is vital to all sectors, we selected four that we've seen from our own qualitative research to be growth areas and in markets that are well represented from both regional and global geographical perspectives.

Demands may differ slightly between countries due to legislation, regulations and budgets, but the sectors that follow often face similar holistic challenges globally – for education, it's about protection and safety of students, whereas for logistics and retail, loss prevention may be more pertinent issues, for instance.

We asked the same three questions for each. Firstly, did the respondent work or carry out work in that sector – if 'no', they were excluded from the remainder of the questions. Installers, integrators and consultants were then asked about the levels of demand they were witnessing for video surveillance projects for each, while the final question asked all relevant professionals to select three examples of video surveillance technology that were most important to that specific sector.

For case studies, news and further insight into each sector, we'd recommend heading to IFSEC Global's specific hub pages for each vertical, with links in the adjacent boxes.

EDUCATION ▶

HEALTHCARE ▶

LOGISTICS ▶

RETAIL ▶



Education

While the education sector is an all-encompassing term for primary and secondary schools (or K12 in the United States), and university/college, the chief aim remains – the protection and welfare of students and staff. Traditionally, this has focused ‘on the campus’, with delivery of security and safety difficult to extend beyond the immediate grounds. However, with technology now providing students with apps to maintain contact with welfare teams, there is a push to extend the delivery outside of the immediate campus environment.¹⁸

In addition, security and estates managers are also tasked with providing adequate protections outside of the traditional school hours. Facilities such as sports halls and pitches are often used by local communities into the late evening, potentially presenting different challenges than in the day.

Protection requires appropriate responses on a regional basis, too. The United States, for instance, faces well-documented challenges from lone actors and firearms, while catering for international students remains a test for universities in the UK.¹⁹ Across the sector, greater collaboration between educational security teams and the public sector such as the local Police will likely be crucial to the improving safety and wellbeing in the coming years.

Our survey provided us with data of 143 professionals who either work, specify or install video surveillance tech in the education sector. Asking installers, integrators and consultants specifically, 32% saw a rising demand for video surveillance in this sphere, while 30% felt that demand is high, but not necessarily increasing. Only 14% said that demand was low, or that they were witnessing a decrease in business in the sector.

Top five requirements for video surveillance tech in education

1	Video surveillance for security
2	Video surveillance for health and safety of staff and students
3	Integration with other physical security systems
4	AI-powered or traditional video analytics
5	Facial recognition

What is video surveillance primarily used for in education, though? Well, video surveillance for security purposes was cited as the most important reason (67%), while surveillance for health and safety of staff and students was also deemed crucial by 45% of respondents.²⁰

The sector also appears to consider tech as an important facet in its overall goals, as a third cited that integration with other physical security systems was important, while traditional video analytics and AI-powered video analytics were selected by 20% and 18% respectively.

Education budgets, certainly in schools, are relatively stretched, with well-documented concerns over rising utility bills in the UK in particular.²¹ Indeed, a survey by the National Governance Association of governors and trustees of state funded schools shows that only 30% reported feeling financially sustainable with current levels of funding and income.²² This may be one reason why more sophisticated AI-based analytics are considered less crucial than traditional video analytics in this sector.



¹⁸ IFSEC Global, “We’ve got the right people, we’ve got the right technology, now, let’s put them together and look after our students” – Collaborative campus safety in Manchester,

<https://www.ifsecglobal.com/security/weve-got-the-right-people-weve-got-the-right-technology-now-lets-put-them-together-and-look-after-our-students-collaborative-campus-saf/>

¹⁹ Darren Chalmers-Stevens for IFSEC Global, Campus gun threat – what’s the right response? <https://www.ifsecglobal.com/critical-conversations/campus-gun-threat-whats-the-right-response/>

²⁰ For clarification, we asked respondents to only select their ‘top three’ choices

²¹ The Economist, Britain’s school budgets are being squeezed by rising energy and wage bills, <https://www.economist.com/britain/2022/09/01/britains-school-budgets-are-being-squeezed-by-rising-energy-and-wage-bills>

²² Education Executive, Balancing the budget is the biggest challenge for schools in 2022, <https://edexec.co.uk/balancing-the-budget-is-the-biggest-challenge-for-schools-in-2022/>

Healthcare

Fundamentally, similar objectives face healthcare security professionals as their counterparts in education – the protection of patients, rather than students, as well as the staff. As Roger Ringham, Chair of the National Association for Healthcare Security (NAHS) pointed to in a recent blog, violence and aggression against staff is on the rise, with 14.3% of staff having experienced at least one incident of physical violence²³ in the UK's National Health Service over the past 12 months.

Top five requirements for video surveillance tech in healthcare

1	Video surveillance for health & safety of staff and patients
2	Video surveillance for security
3	Integration with other security and building management systems
4	AI-powered or traditional analytics
5	4K/HD surveillance

Regulatory change, investment in resources and training for security professionals, are all considered to be key to combatting issues, but technology such as video surveillance has a role to play. Clearly there is an awareness of this in the sector, with 35% of installers and consultants citing that they were witnessing 'rising demand' in the healthcare sector for video projects, while another 40% said that though it wasn't increasing, demand remains high.

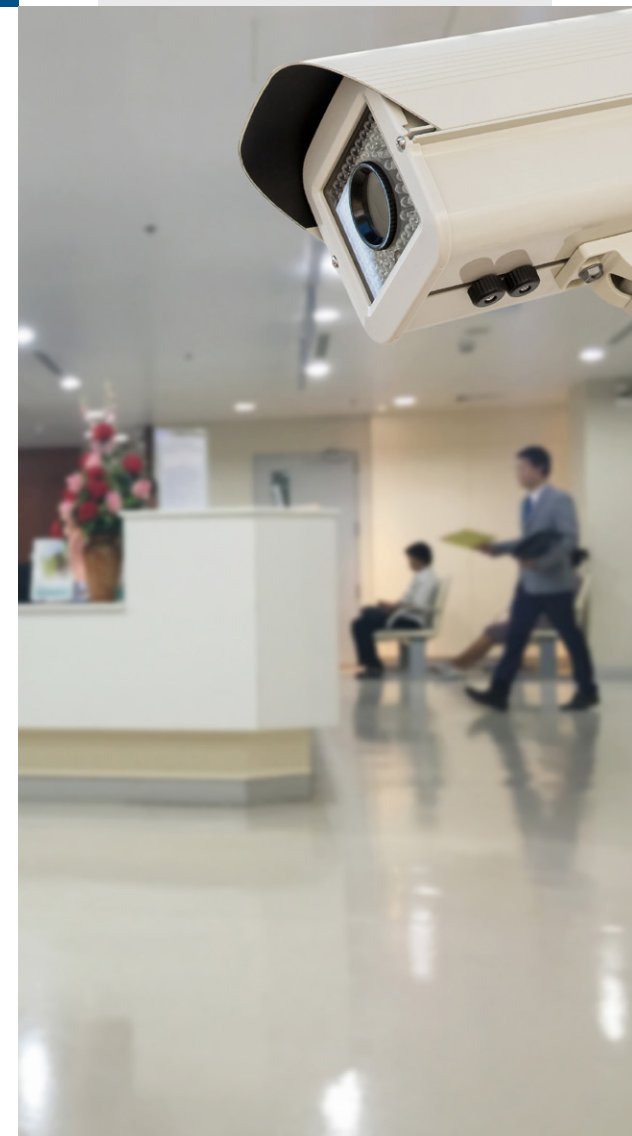
The health and safety of staff and patients was deemed the most critical reason for using video tech in the sector (60%), closely followed by security purposes (56%). Once again, the integration with other physical security systems was deemed important, this time by 37% of respondents. The ability for security systems to work alongside each other is often vital for a healthcare site operating efficiently – interlinked audio and voice alarm devices with cameras support professionals to relay critical information around sites that may not be easy to physically access, for instance.

AI-powered devices were deemed more important to the healthcare sector than traditional analytics, according to our data. Instances of AI being used to detect slips and falls in social care settings may provide users with crucial alerts they may have otherwise missed – potentially saving precious response time.

Logistics

Security staff in the logistics sector are faced with myriad challenges, and in particular those involved in the transportation and storage of vaccinations during the COVID pandemic were put under significant pressure throughout the past few years.²⁴

Again, we can see the demand for video surveillance projects in the sector, with 62% citing that it was either rising, or at least remained high. Only 10% believe that demand is relatively low or decreasing, in contrast.



²³ Roger Ringham for IFSEC Global, The obstacles to staff safety and wellbeing in the NHS, <https://www.ifsecglobal.com/physical-security/the-obstacles-to-staff-safety-and-wellbeing-in-the-nhs/>

²⁴ IFSEC Global, Global COVID vaccination programme fraught with security challenges, <https://www.ifsecglobal.com/global/covid-vaccination-programme-fraught-with-security-challenges/>

Top five requirements for video surveillance tech in logistics

1	Surveillance for loss prevention
2	Integration with other physical security systems
3	AI-powered video analytics
4	Surveillance for health and safety of staff
5	Occupancy monitoring

Marking a notable difference from healthcare and education, those installing or operating surveillance cameras in the logistics sector selected 'surveillance for loss prevention' as the most important reason for implementing the tech. With over half citing this reason (54%) and another 45% choosing 'integration with other physical security systems', there is a clear security purpose for security operators in logistics.

Goods in transit can be protected by in-cab surveillance systems or cameras set up at ports, for instance, with a report in 2021 highlighting that widespread congestion in ports and inland facilities has led to increased opportunity for offenders.²⁵ AI-powered analytics that can cover large areas and spot motion detection, or classify unusual behaviours, may also support in preventing the loss of goods, with 35% of professionals noting that these are important to the logistics and warehousing sector.

Where many goods are located all in one place but spread across a wide area, such as at ports, guarding operations

are made more challenging. Vandal resistant cameras were marked as important to the sector by 14% of respondents, while another 14% selected 4K/HD surveillance – perhaps due to the need to spot trespassers from long distances.

Retail

The retail sector has perhaps been the most widely cited use-case for AI and video analytics software applications in video surveillance systems. Proponents point to the fact that cameras can do so much more than act as security deterrents in 2022, and can provide retail stores in particular with substantial business operational insight.

Cameras with embedded analytics can spot patterns in shoppers' movements via footfall analysis and loitering detection, while behavioural analytics can identify areas of stores where efficiencies or flow could be improved to help drive revenue at the point of sale. This is perhaps why such options were cited by 13% (certainly more so than the comparative sectors) of professionals, and 42% selected AI-powered video analytics.

Top five requirements for video surveillance tech in retail

1	Integration with other physical security systems
2	Surveillance for loss prevention
3	AI-powered analytics
4	Facial recognition
5	Integration with other building management systems



²⁵ Loss Prevention Magazine, Supply chain congestion increases theft of cargo theft, <https://losspreventionmedia.com/supply-chain-congestion-increases-threat-of-cargo-theft/>

Notably, however, security remains a key concern, and it's of little surprise that 45% of respondents still believe surveillance for loss prevention in stores is in the top three reasons for installing CCTV, while another 50% selected integration with other security systems to ensure holistic protection. AI and video analytics can complement this, of course, where high-definition cameras can detect shoplifting in real time and machine learning algorithms predict patterns of behaviour related to concealment of items.²⁶

Notably, a quarter selected facial recognition in their top three reasons. The arguments for and against the use of video surveillance in public spaces such as retail outlets remain divisive. UK food and beverage retailer Co-Op, for instance, installed a facial recognition system in 35 of its stores this year, designed to detect those on a 'watchlist'. In response, a privacy campaigner group raised the complaint to the Information Commissioner's Office (ICO) arguing that the retailer's use of "live facial recognition is Orwellian in the extreme, highly likely to be unlawful, and must be immediately stopped."²⁷

Facial recognition has its benefits, but the debate is nuanced, particularly in areas which directly impact on the public such as in retail and regions where data privacy regulations are in place. Its use as a potential crime prevention tool may be 'music to the ears' of store security operators and managers, but from a legal perspective and in practice, it remains a complex compliance challenge.²⁸

Affordable deep-learning analytics for smaller businesses

The licence-free, 4-channel AI Retail Box is a simple add-on appliance that meets the in-store and customer intelligence needs of small stores with at-a-glance dashboards and tools including people counting, queue monitoring, heat mapping and analytics reports. It provides data and insights to help retailers continuously improve promotions, merchandising, store layouts and staff deployments.

Smaller businesses can also reduce false alarms and enhance security with the DV-1304-A AI Box, and avoid upgrading cameras to benefit from tools including line cross, object, loitering, intrusion and facial detection.



IDIS AI Box for Retail

²⁶ Hunter Seymour for IFSEC Global, Retail Theft: The growing frontline threat in a cost-of-living squeeze? <https://www.ifsecglobal.com/physical-security/retail-theft-the-growing-frontline-threat-in-a-cost-of-living-squeeze/>

²⁷ IFSEC Global, UK retailer Co-Op's use of facial recognition cameras faces legal challenge from privacy campaigners, <https://www.ifsecglobal.com/video-surveillance/co-op-facial-recognition-cameras-face-legal-challenge-privacy-data-protection/>

²⁸ IFSEC Global, Automatic Facial Recognition – The debate in 2022, <https://www.ifsecglobal.com/surveillance/automatic-facial-recognition-the-debate-in-2022/>

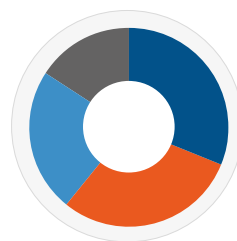
Wider economic and geopolitical challenges: The impact on video surveillance

Despite much of the world returning to a semblance of 'post-COVID normality' in 2022 – albeit at different stages – the wider market outlook remains challenging. The effects of emergency measures such as the furlough scheme and wider impact on national debt remain to be seen, while fresh challenges have arisen, further disrupting any hope of a speedy recovery for national economies and the international marketplace.

The UK, where a significant number of our respondents are based, is certainly facing its own difficulties at present. At the time of writing, several factors – from the war in Ukraine through to supply chain issues, the rising cost of living and government policies – have contributed to the value of the pound dropping sharply, as interest rates rise and pressure is put on organisations of all sizes, both to manage their own costs and to ensure the security and welfare of their employees.

How robust is the market?

However, as we found in both the 2020 and 2021 Video Surveillance reports, the physical security market tends to be relatively robust. Indeed, last year almost a quarter (22%) of respondents claimed they didn't see a drop-off in business throughout the pandemic.²⁹ This assessment has been supported from this year's cohort, too. 20% of respondents said that they hadn't seen an impact to their, or their customers' video surveillance upgrade plans, despite a global pandemic and wider economic challenges.



Has the global pandemic, or wider economic challenges affected video surveillance upgrade plans?

- (20%) No, carried on as normal
- (19%) No, it's being considered but hasn't affected the physical security budget/projects
- (50%) Yes, it's caused a reassessment and delays, but projects are still happening
- (10%) Yes, upgrade plans/projects have been cancelled as a direct result

²⁹ IFSEC Global, The Video Surveillance Report 2021, <https://www.ifsecglobal.com/resources-1/the-video-surveillance-report-2021/>

While some of these answers may encompass those end-users who didn't have upgrade plans in the first place, another 19% cited that while economic challenges were being considered, they hadn't fundamentally affected or changed the physical security budget or projects in place. Though one in 10 did cite that upgrade plans or projects had been cancelled as a direct result, it would still be reasonable to suggest the video surveillance market has been quite robust over the last few years.

Projects have not been completely disaffected, however. 50% of respondents cited that while projects were still taking place, they had been subject to reassessments or delays. Myriad reasons could lay behind disruption, of course, but a clear trend is the impact of the global chipset shortage.

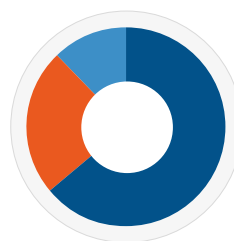
Component shortages continue to disrupt

A phenomenon that relates to the supply of semiconductors, any industry reliant on chipsets – think the majority of new video surveillance cameras as the obvious example – has likely felt the effects of shortages in the past 24 months. Knock-on effects have included delays of goods, manufacturers overstocking in an effort to 'pad' their supplies, as well being a driver behind global price inflation for affected products.³⁰

Last year's report saw 48% of professionals answering 'yes' to whether they'd seen the impact of the chipset shortage, while 33% said 'no' and 19% 'weren't aware of a chipset shortage'.³¹ In comparison, 64% of this year's respondents answered 'yes' to the same question, 24% no and only 12% cited they weren't aware. We can see significant differences in just a 12-month period then, demonstrating the growing

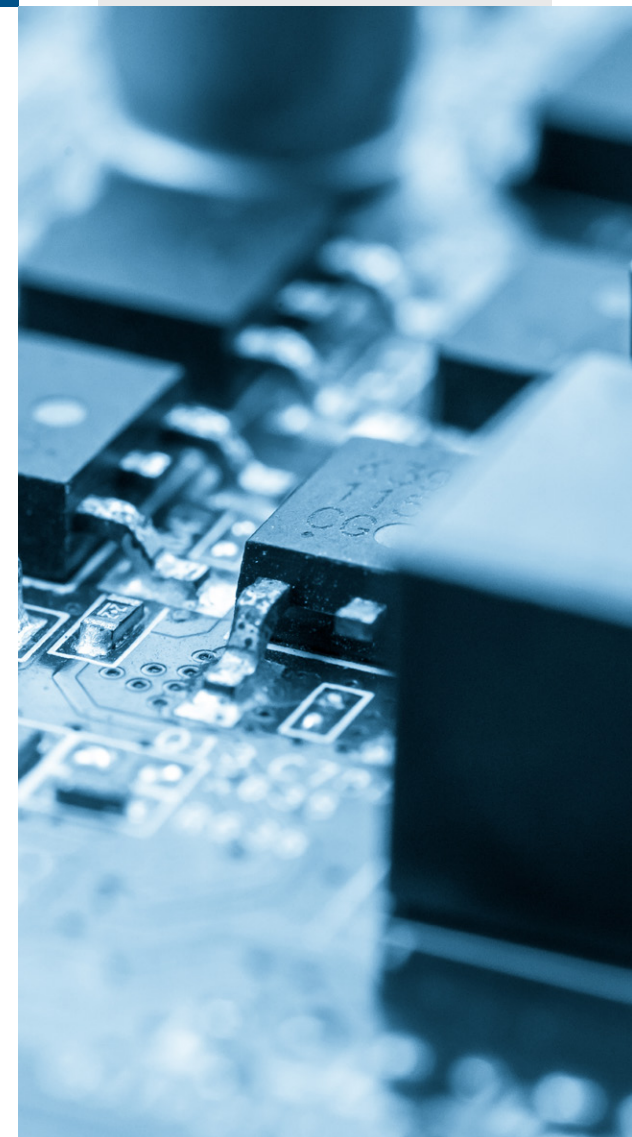
impact that a globalised tech market – particularly one reliant on specific geographical regions – can have on video surveillance projects.³²

While there is a belief that the shortage will begin to ease throughout the second half of 2022, the knock-on effects will likely continue for some time.



Have you seen any impact of the global chipset shortage on the supply/availability of surveillance cameras or associated tech?

- (64%) Yes
- (24%) No
- (12%) Wasn't aware of a global chipset shortage



³⁰ Techradar, Global chipset shortage: what is it, why is it happening, and when will it end? <https://www.techradar.com/news/global-chip-shortage>

³¹ IFSEC Global, The Video Surveillance Report 2021, <https://www.ifsecglobal.com/resources-1/the-video-surveillance-report-2021/>

³² Taiwan is perceived to be one of the key areas of production for chipsets, being home to the Taiwan Semiconductor Manufacturing Company. Alongside political tensions with China, a series of droughts in the region affected the production facilities according to reports.

The China question – A changing market outlook?

Another issue that hasn't disappeared since last year's report is the China question. Indeed, further concerns have been raised in the UK since, notably by the Surveillance Camera Commissioner's Office, as well as by a cross-party group of MPs (Members of Parliament), calling for a ban on Chinese video surveillance tools.³³ Meanwhile, in the United States, the Secure Equipment Act 2021 was passed into law in December 2021, which "solidifies the authority of the Federal Communications Commission (FCC) to deny equipment authorised from its 'Covered List' entities".³⁴

Have concerns continued to affect the wider security industry? Almost a quarter (23%) responded that they would continue to use, sell or install Chinese surveillance tech (a little lower than last year's 27%), while 13% answered that they never installed the equipment anyway and 15% remained unsure.

The concerns raised by governments and wider media outlets do appear to be influencing a significant number of security, facilities and IT professionals, though. The most popular answer was 'Yes – there are increased concerns' (30%), suggesting that these respondents may still be using them, but are considering switching or at least using them a little less. 10% answered that they were planning to phase out selling, installing or using such technology, while another 8% cited they had stopped using Chinese-based surveillance technology altogether.

"There's little doubt the NDAA, and the anticipated Secure Equipment Act have influenced purchasing decisions beyond the United States. Customers from banks, hotel chains, schools, and multinational companies to those with links to the US or with American expansion plans are opting for NDAA-compliant equipment. There is also awareness among buyers that the UK and European Union could introduce similar standards, so ensuring futureproof compliance of solutions is becoming an important consideration in purchasing decisions," notes James Min, Managing Director, IDIS Europe.

Brands from China remain some of the most dominant and competitively priced in the market, but it would appear that rising geopolitical tensions, concerns over privacy and questions relating to human rights, may have an impact on the outlook of the video surveillance marketplace in the coming years. ■



³³ Forbes, UK lawmakers call for ban on Chinese surveillance tools, <https://www.forbes.com/sites/emmawoolacott/2022/07/05/uk-lawmakers-call-for-ban-on-chinese-surveillance-tools/?sh=6ff8f4063c57>

³⁴ Forbes, Secure Equipment Act Becomes Law, <https://www.forbes.com/sites/roslynlayton/2021/12/01/secure-equipment-act-becomes-law/?sh=68ad26196247>