# The video surveillance report 2017

## Cybersecurity, open platforms, 4K, low-light cameras, video analytics and warranties

Sponsored by IDIS

Sponsored by IDIS A trend report from IFSEC Global
Connecting the Security and Fire communities

# 1. Introduction

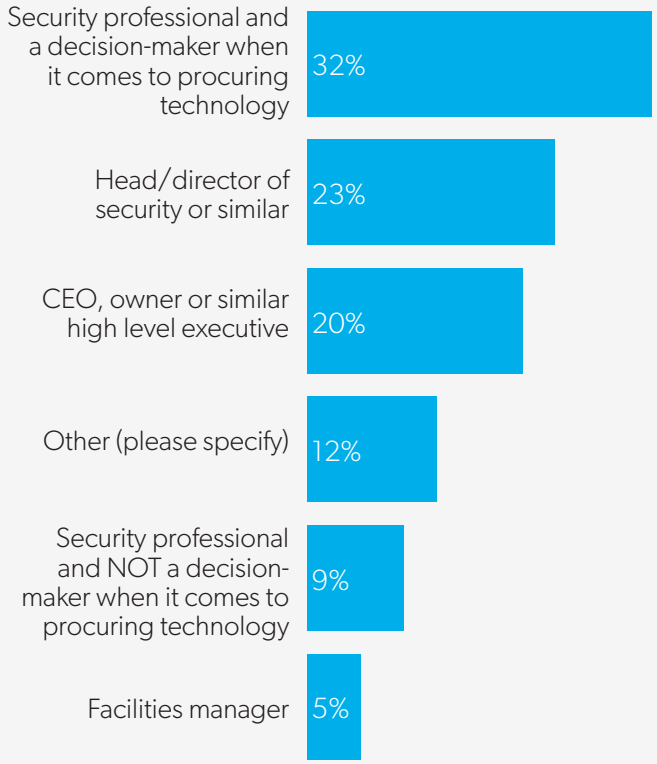
*The Video Surveillance Report 2017* builds on the success of two previous reports in 2015 and 2016 on the same subject – also sponsored, like this report, by global surveillance leader IDIS, the largest manufacturer in South Korea. In 2015, Video surveillance: market trends and expectations provided a snapshot of systems installed around the world, the factors underpinning procurement decisions and how control rooms used CCTV systems. The video surveillance Report 2016: security needs and plug and play, meanwhile, focused on upgrade motivations, the security needs of surveillance systems as shaped by the physical environment, the threats posed to people, data and assets, what security professionals thought about plug-and-play systems and which cutting-edge features they valued most highly.

This time round there was one subject in particular that we'd have been neglectful to ignore: cybersecurity. Information security once seemed a different world altogether to the realm inhabited by physical security professionals. But any demarcation between the two disciplines has now been emphatically demolished. Integration with other buildings systems, a spate of breaches – including the hijacking of network cameras during the 2017 presidential inauguration – and the spectre of more punitive fines for data breaches under the forthcoming EU data protection law (the GDPR), is sharpening minds across the supply chain as vendors, installers and security professionals scramble to strengthen their cyber defences.

With this in mind, some of our findings on page 6 make for interesting reading.

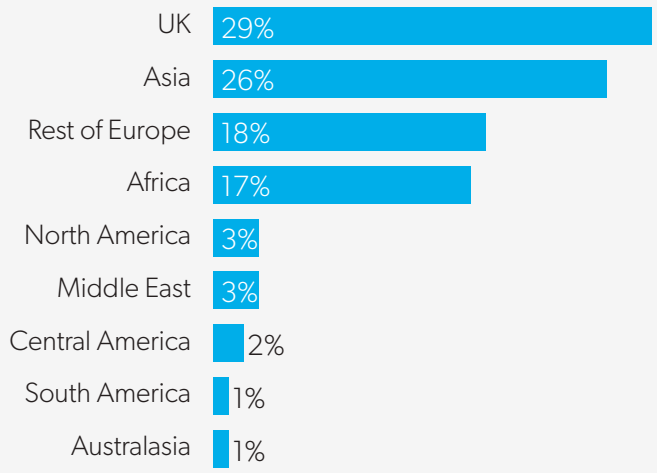
## CONTENTS

## Which of the following best describes your level of responsibility?*




*241 respondents

## In which region are you based?*

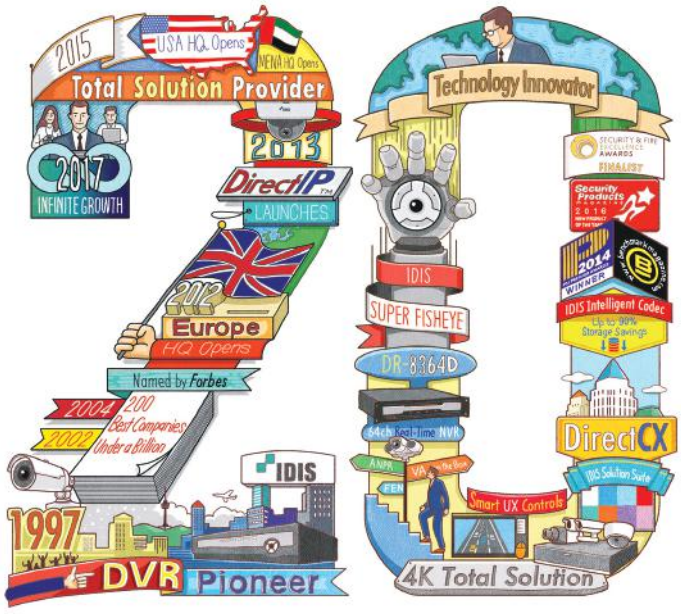



*241 respondents

In a wide-ranging survey, we also polled the industry extensively on the value of warranties in general and extended warranties in particular. Do long warranties suggest the vendor has faith in the reliability of their product – or could it even signal the very opposite?

In terms of the tech, we revisited the topic of video analytics (VA), including the prevalence of VA on the edge. There were also questions on the prevalence of ultra-low light cameras versus thermal cameras, demand for 4K cameras and the prevalence of analogue versus IP systems.

Once again, our sponsors, IDIS, provides commentary throughout, with notable comments from survey respondents also featured. The survey was completed by security professionals with various levels of authority, in organisations ranging in size from sub-50 employees to more than 1,000, in a variety of verticals from around the world (though the UK accounted for the largest proportion).




**IDIS 20th Anniversary**

**Celebrating Two Decades of Innovation**

Learn more of the IDIS story at www.idisglobal.com/idis20

## About the sponsor: IDIS

IDIS is a global security company that designs, develops, manufactures and delivers surveillance solutions for a wide range of commercial and public sector markets. As the largest video surveillance manufacturer in South Korea, headquartered just outside of Seoul, and operating across 50 countries and 100+ strategic partners, IDIS is a world-leading total solution provider with more than two million recorders installed worldwide and over 16.5 million cameras utilising IDIS technology.

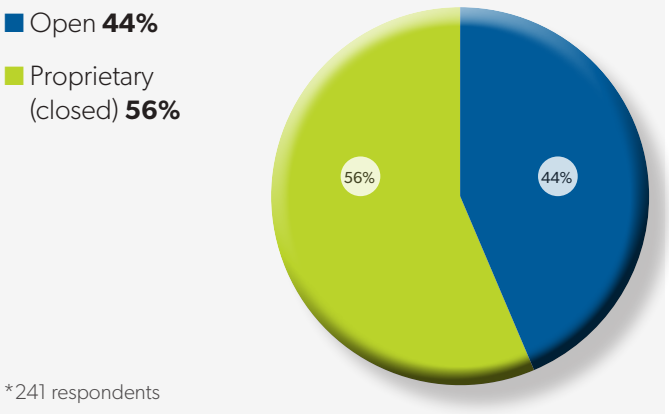
Celebrating two decades of innovation, IDIS has met the needs of an increasingly demanding security landscape since its founding in 1997. IDIS provides the benefit of an end-to-end, highest-quality surveillance solution at a low total cost of ownership. IDIS delivers innovation that is flexible and scalable, able to meet every surveillance need – all with unrivalled performance, quality and low total cost of ownership.

# 2. The rise of open platforms

With end users increasingly prizing integration between disparate systems and the technology becoming more software-driven, much of the security industry has embraced open platforms.

This trend mirrors the evolution of other building technologies. In The smart buildings report 2017 we wrote that "the building control industry, like most other high-tech sectors, was born in a closed source world. Systems were built on proprietary hardware and software stacks, leading to a highly fractured, disparate ecosystem of quasi-intelligent systems. The demand for greater interoperability prompted the industry to move away from proprietary systems to a much more open architecture." The same drivers very much apply to surveillance systems.

## Is your CCTV system on an open platform or proprietary (closed) system?*




*241 respondents

**The direction of travel is clear: growing numbers of vendors are abandoning the proprietary model**

Nevertheless, plenty of proprietary systems are still in operation. Indeed, they account for the majority of installed systems at 56%. Yet for those survey respondents whose systems were installed in the last five years, this figure was 14 percentage points lower than for older systems, at 52% against 66%. The direction of travel is clear: growing numbers of vendors are abandoning the proprietary model, so it's easy to imagine this far-from-overwhelming overall majority being overturned in the coming years.

### Integration

Nearly half (48%) of security professionals are "integrating – or plan to integrate – CCTV with other systems to generate collective business intelligence from data from numerous systems including IoT sensors etc".

Respondents with plug-and-play systems were marginally more likely to have such integration plans: 50% against 47% of those with other types of systems. This contradicts

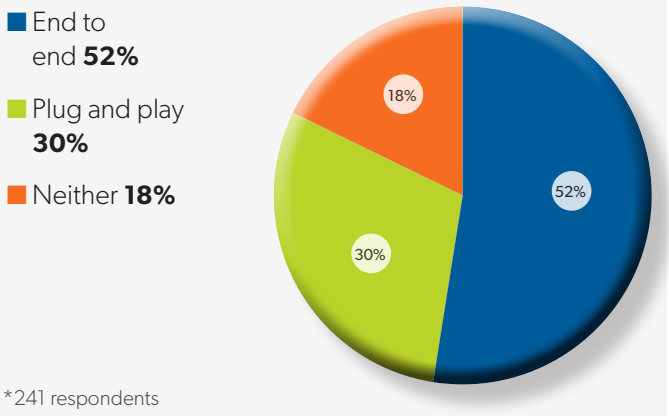

## View from the vendor

"End-to-end systems will always have their place, particularly for smaller surveillance applications. That's why there's great demand for DirectIP™ in the SME space as well as in retail, where and organisations might have hundreds of stores up and down the country. End-to-end systems are fast and simple to install and low maintenance and can indeed simply integrate with other security systems such as access control and intruder as well as ONVIF-compliant cameras from other manufacturers.

"At the same IDIS recognised the growth of open platform solutions, particularly for larger deployments and developed our enterprise-level video management software (VMS) IDIS Solution Suite, which is a truly open platform. It allows of the integration of a myriad of ONVIF-compatible cameras as well as legacy analogue cameras and provides the flexibility and scalability to integrate with other security and back-office systems." **Brian Song**, *managing director, IDIS Europe*

the assertion posed in last year's survey – with which one in three agreed – that "plug and play is problematic when integrating CCTV with other security tech."

**Is your system an end-to-end system from a single manufacturer or plug and play?***




*241 respondents

Integrating different building systems onto a single network to collect, share, analyse and automatically respond to data is effectively the definition of the term 'smart buildings'. Global spending on smart-building technology was forecast to grow from $7bn in 2015 to $17.4bn by 2019 by IDC Insights *(Business Strategy: Global Smart Building Technology Spending 2015–2019 Forecast)*.

In our recent trend report on smart buildings we asked hundreds of security professionals, facilities managers and others involved in building management which of their building functions they would describe as having 'smart' functionality. The most commonly chosen option was CCTV, with 67%, which suggests that the industry is at the forefront when it comes to integration and harnessing big data.

# 3. Cybersecurity in the age of convergence

As a long-term trend crime rates have fallen steadily in most categories across the western world since the 1970s. Whatever its role as a deterrent in this success story, CCTV has certainly helped to identify and convict criminals – and with growing effectiveness as technology has improved.

But surveillance systems are now potential facilitators for a comparatively low risk, high reward class of crime that is growing exponentially. On October 2016, more than a million security cameras were hijacked and used as a bridgehead to bring down security website KrebsOnSecurity.com with a distributed denial of service (DDoS) attack. Then in January 2017, CCTV cameras in Washington DC were hacked eight days before the presidential inauguration.

Then there's the General Data Protection Regulation (GDPR). Coming into force across the EU from 25 May 2018, the GDPR stiffens penalties for data protection violations – including shortcomings in data security.

And yet: 41% of those with IP systems professed to not being at all concerned about their CCTV system's potential vulnerabilities. Are they being complacent? "Our CCTV systems operate on a separate network with no internet/wifi access, so we are relatively safe from intrusion," explained a senior security professional employed in the US hospitality trade. A South-Africa-based respondent charged with protecting a business in the IT/digital sector said they had every confidence in their preparedness: "I have a good grasp of cybersecurity implications and know the system we have is correctly installed with https setups and correct firewalling to avoid DDoS and botnet attacks." More succinctly, another respondent suggested that "if your protection from cyber-attacks is robust, then there is less to worry [about]."

### View from the vendor

"IDIS has seen more and more organisations wanting to move away from implementing IP video surveillance on their corporate network due to security concerns and the rise in data theft. The IDIS Total Solution uses a dedicated IP camera subnet, separate from a customer's corporate network, separating the video traffic and making it very difficult to establish an unauthorised connection into a corporate network. At IDIS, we also educate our installers and integration partners to design a physically separate network, or to configure a dedicated network by VLAN."
**Brian Song**, *managing director, IDIS Europe*

**"The lack of technical knowledge of physical security service providers on IP-based systems and IT platforms provides an ideal opportunity for cyber-attacks." Technical advisor on PSIM in the financial sector**

Research conducted for cloud-based surveillance company Cloudview found that both traditional DVR-based systems and cloud-based systems were vulnerable to malicious breaches. During tests, five routers, DVRs and IP cameras running the latest software were connected to the internet. One device was breached within minutes, while another two fell under the control of an unknown attacker inside 24 hours. A fourth became unstable and completely inoperable.

### View from the vendor

"It's important that organisations look to security technologies that make hacking much more difficult. IDIS devices, such as NVRs, use a proprietary embedded Linux – ie not off-the-shelf – on which only authorised network modules can run, and IDIS does not allow any third-party apps to run inside the IP camera. Since we leverage proprietary protocols, this makes them very difficult to exploit. IDIS has also developed proprietary file structures, whereas some manufacturers use Windows or off-the-shelf Linux, another example of how we harden network resilience. Even a common network module, such as our HTTP/HTTPS server, is a proprietary implementation, which will make many known attacks ineffective.

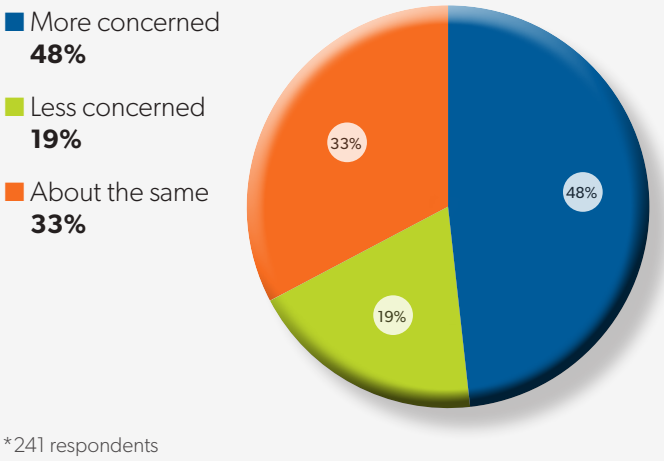
"IDIS also uses industry standard SSL/TLS when communicating across a network as well as the encryption of login details, IP filtering, IEEE 801.1x and TLS/SMTP.

"Many security professionals have concerns that manufacturers can access an end user's system. With IDIS technology, users' passwords are encrypted. For example, if an administrative account password for an NVR is lost, then there is no way to reset it, even by IDIS engineers who designed the system. Unlike other manufacturers, IDIS does not use 'back doors'. These 'back doors' are typically used to gain access and provide remote customer support. However, they can also spur fears of espionage. There are recovery options with IDIS systems, but these need to be set up by the installer when the system is implemented. So, for the sake of network security, IDIS cannot access any of its own installed systems."
**Brian Song**, *managing director, IDIS Europe*

The research found that both DVR-based and cloud video solutions used port forwarding and Dynamic DNS, creating vulnerabilities, while the former issued too few firmware updates and often left 'back doors' open. Other problems included poor use of secure protocols, a lack of encryption, substandard cookie security and insecure user and credential management.

But vendors are waking up to the problem if their recent marketing output is any barometer and cybersecurity is now a major talking point elsewhere in the supply chain. Nearly half (48%) of security professionals polled said they were more concerned about the cybersecurity threat than they were two years ago, with only 19% claiming to be less worried. "With the media coverage of cybersecurity issues and hacking of cheap Chinese imports, I believe there is more concern than there was 18 months ago," noted one UK-based professional.

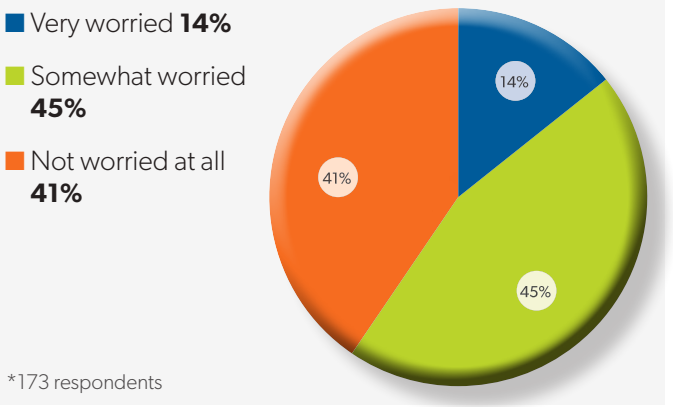
## Are you more or less concerned about the hacking threat to CCTV than you were two years ago?*




*241 respondents

How to explain the 19% who were less concerned? The obvious answer is that they've recently bolstered their cybersecurity defences. Filter the data to those who installed or substantively upgraded their systems in the last five years and there was indeed less concern about the cybersecurity threat than those with older systems: 14% with newer systems were 'very' worried (compared to 16% of those with older systems), 42% were 'somewhat' worried (versus 54%) and 44% professed to not be worried at all (versus 30%).

## How worried are you about your CCTV system's vulnerabilities?*




*173 respondents

Professionals employed in sectors we could reasonably define as critical national infrastructure – government, healthcare, industrial/mining, transport, utilities and agriculture – were more likely to be worried about their systems' cyber vulnerabilities (66% were at least somewhat worried compared to 58% for other sectors) and to be more concerned about the cyber threat than two years ago (52% being more concerned and 5% less; versus 47% and 21% for other sectors).

## View from the vendor

"Network security breaches are rarely caused by the exploitation of encryption technology weaknesses. Rather, they are more often the result of human factors, such as not enforcing network security best practices. For example, when an organisation deploys a VMS with 300 IP cameras, the installer needs to manage around 300 IP addresses, 300 MAC addresses and 300 login credentials for each IP device. This creates a high level of complexity to manage throughout the whole system lifecycle.

"Most IP cameras now ask users to change login credentials at the first login, with upper and lower-case letters, numbers and special characters. However, when you have 300 separate logins, installers often do one of two things: use a single login for all 300 cameras or create separate logins and record them in an Excel spreadsheet – both of which make the system very easy to breach.

"IDIS has eliminated this complexity and designed its Total Solution with network security in mind. DirectIP utilises true plug-and-play with the implicit pairing of devices, and in doing so, the system reduces the amount of information that is managed.

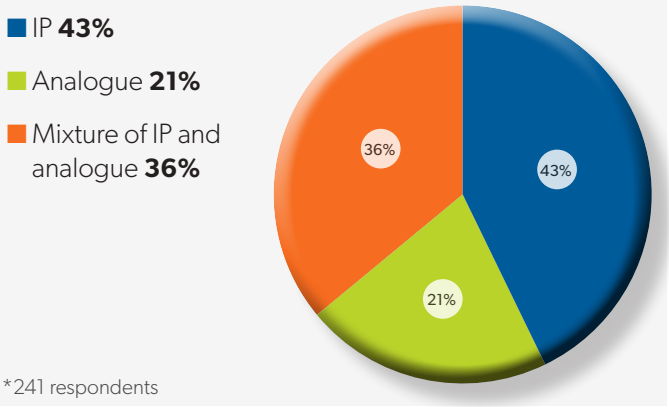
"The registration (ie pairing) of IDIS IP cameras and network video recorders (NVRs) is implicit and hidden from users. This ensures that installers do not have to manage the device, minimising the level of human risk during implementation. This can easily reduce complexity 30-60-fold. A user only needs to manage one IP device, the NVR. At IDIS, we call this 'manageable complexity'. It becomes an even more useful concept for large applications or as an organisation's system grows." **Brian Song**, *managing director, IDIS Europe*

Respondents working for organisations in the IT/digital tech/cybersecurity fields were more likely to "consider reverting to a closed protocol or analogue system from an alternative brand"' if they "fell victim to a costly cyber-attack" (46% saying 'yes' compared to 30% for all other sectors) but not appreciably more worried about their system's vulnerabilities than they were two years ago.

**4. Analogue systems: a more secure alternative?**

More than a decade since the dawn of the IP age, analogue cameras are still installed as part of a slim majority – 57% – of systems, with 21% of systems having exclusively analogue cameras. However, filter the results to systems installed in the last five years and the picture is rather different; 49% of systems feature analogue systems, of which only 15% are exclusively analogue, against 79% and 33% respectively for older systems.

### Is your system analogue or IP?*




*241 respondents

Given that you can now connect a toaster, a fridge or even a hairbrush to the internet, it might seem quaint to outsiders that the humble analogue camera remains prevalent in the physical security industry. And this isn't just legacy systems that are yet to be upgraded; revenues from global network camera sales only overtook those of analogue cameras in 2014 (IHS Markit). Our 2016 video surveillance report also revealed, it is worth noting, that 56% of security professionals without an HD analogue solution said they would consider switching to one if it were cost-effective, simple or leveraged existing coaxial cables.

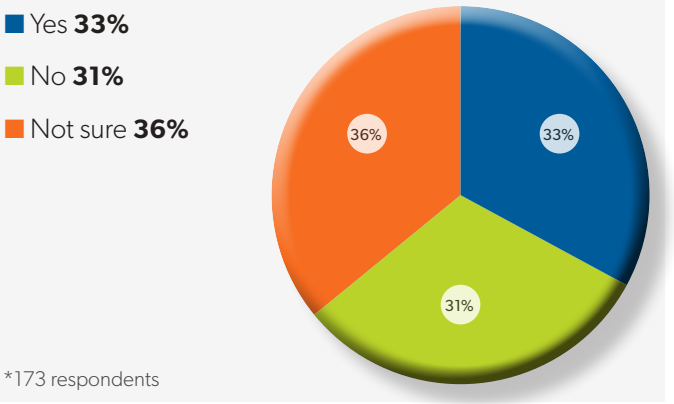

### View from the vendor

"These findings correspond with the successful launch two years ago of IDIS DirectCX, an advanced over coax solution based on high definition transfer video interface (HD-TVI) technology that incorporates IDIS expert imaging processing to deliver incredibly high-performance HD recording at a low price point. The results are speaking for themselves, with one IDIS distributor selling a significant amount of IDIS DirectCX, reporting strong demand not just from organisations wanting to leverage existing coaxial cabling, but also from small regional installers that are still happier recommending analogue since they still don't fully understand that IP or plug-and-play solutions like IDIS DirectIP are just as easy to implement, operate and maintain as analogue." **Brian Song**, *managing director, IDIS Europe*

Almost one in three respondents (33%) with IP cameras said they would consider reverting to a closed protocol or analogue system if they fell victim to a costly cyber-attack. Whatever the benefits of IP cameras – and these are manifold – many security professionals are clearly concerned about the potential security risk.

Simon Lambert, an engineer and CCTV consultant, has suggested that "people who appear to be 'firmly attached to their analogue counterparts' are the ones not easily hoodwinked. They know that, in reality, IP cameras are clearly not essential if you want remote viewing." Speaking to IFSEC Global, he also noted that "pretty much all analogue CCTV has been recorded digitally for years now, so it could easily be connected to the internet."

### If you fell victim to a costly cyber-attack, would you consider switching to a closed protocol or analogue system from an alternative brand?*



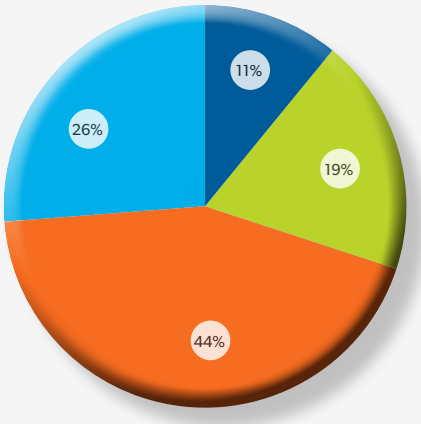

*173 respondents

# 4. Cutting-edge technologies

**4K resolution**

Just 11% of respondents already enjoy 4K resolution from their network cameras. However, a significant majority (71%) of the rest said they expected to eventually need it, with 49% intending to get 4K only when prices fall low enough. A UK-based security professional involved in procurement decisions said: "4K is the next evolution but costs need to reflect what customers want to pay and invest in their infrastructure." With prices falling, we can perhaps expect to see that 11% figure rise sharply in the coming years.

## Do you think you need 4K?*




- Already have it… **11%**
- Yes – it's important to achieving our security goals and we plan to upgrade ASAP **19%**
- Yes – but only when prices drop to low enough levels **44%**
- No – we probably won't ever need 4K for any security application **26%**

*188 respondents


Not everyone is so readily swayed by the merits of higher resolutions in every instance. "At IFSEC [the UK security trade show] there are 30 companies all selling the same systems and claiming theirs is best," said one sceptical company director. "What actually works? 4K is only any use if people want more than a visual deterrent."

> **One senior security professional suggested that buyers must consider "context, relevance and never [upgrade simply] for the sake of [better] technology"**

As ever, whether you need 4K ultimately comes down to your operational requirements. "The purpose of CCTV must be clearly defined from the outset," CCTV consultant Simon Lambert has told IFSEC Global. "Sometimes the most expensive solution may be the most inappropriate, because if you just need to see whether the back door is open when somebody is having a crafty ciggy, then a 29 megapixel camera is wholly inappropriate." Expressing similar sentiments, one South Africa-based security professional who completed the survey said: "It is important to understand what the camera's job is and how the camera model and megapixel rating affects the required delivery. In some cases a standard 4CIF analogue camera will do the job just fine." A senior security professional based in Singapore suggested that buyers must consider "context, relevance and never [upgrade simply] for the sake of [better] technology."

**Lowlight versus thermal cameras**

Around a third (32%) of those polled in our survey already use lowlight cameras while a further 42% intend to at some point. One in four (25%) still prefer to use thermal cameras for their particular environment.

## View from the vendor

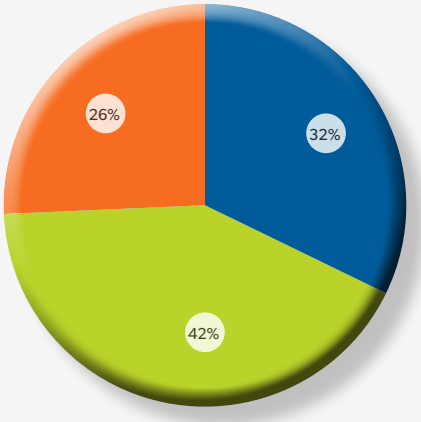
"For certain, 4K is not suitable for every application, yet 4K cameras can deliver four times more coverage that FHD1080p. This is incredibly useful for covering vast areas that require sharp, accurate and powerful image analysis and is therefore particularly well suited to high security environments such as airports or stadiums. Like many other manufacturers, IDIS launched over two years ago a full 4K line up that provides a mix of 4K technology that includes NVRs, cameras and 4K monitors. We have seen strong demand in mission-critical security operations like utilities and transport, but certainly not mass adoption.

"Many people already have 4K televisions, but most broadcasters are yet to deliver 4K programming to our screens. Once that happens, we may well see more security operatives demanding the same resolution from their surveillance systems as they enjoy from their TV, which would follow the trend of demand for HD." **Brian Song**, *managing director, IDIS Europe*

Of course, if you need to capture fine details by daytime but also require motion detection capabilities in complete darkness at night – and you have a sizeable budget – you could have the best of both worlds and cover a scene with both thermal and lowlight cameras.

## Do you expect to use ultra-low light cameras instead of thermal imaging cameras?*

- Yes – we already use ultra-low light cameras **32%**
- Yes – we intend to use low-light cameras **42%**
- No – thermal imaging will always have its place **26%**




*188 respondents

### A grudge purchase no longer: Video analytics

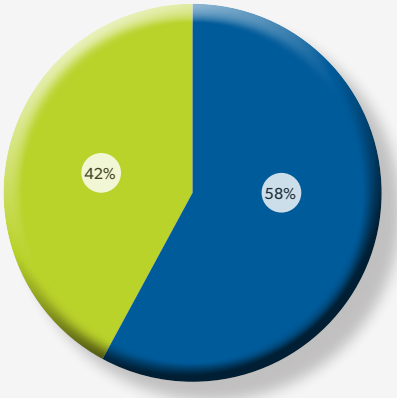
"Video surveillance is no longer a 'grudge purchase' thanks to video analytics and other cutting-edge functionality," according to around a third (34%) of respondents.

When it comes to securing funding for upgrades, it was once impossible to measure the return on investment of CCTV. Heads of security couldn't present to their board the costs avoided because would-be thieves were deterred or caught by security cameras. It's impossible to know the outcome of events that didn't happen or unfold in a different way.

Video analytics, however, was a game-changer. Automating the monitoring process – encompassing motion and intrusion detection, people tracking, facial recognition, recognising loitering and raising alerts/alarms, among other things – CCTV software could do the job both more effectively and at a lower cost than security guards. Software got neither tired nor distracted and didn't demand a salary – a much easier sell when seeking sign-off on a technology upgrade.

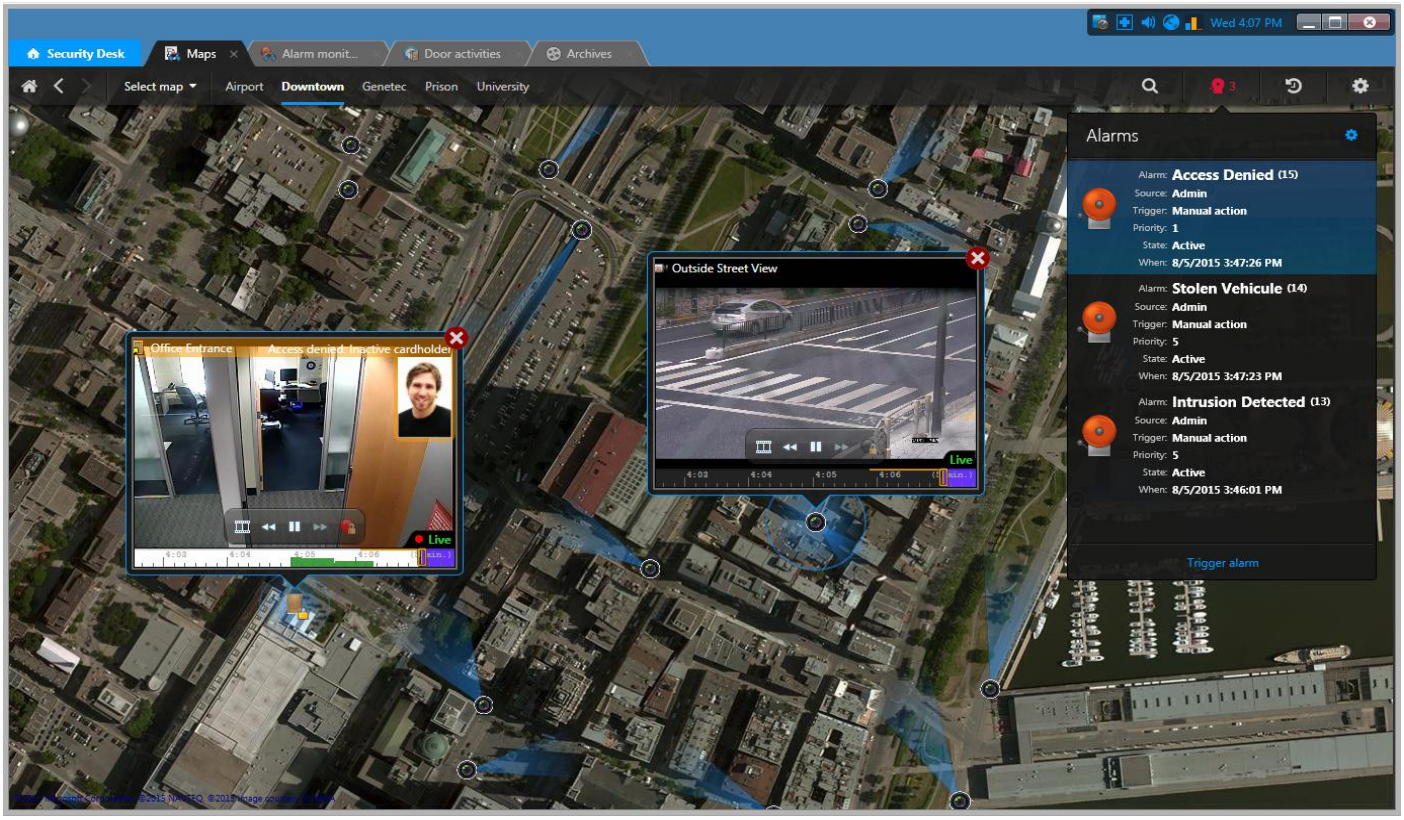
## Do you have experience of using or implementing video analytics?*

- Yes **58%**
- No **42%**




*188 respondents

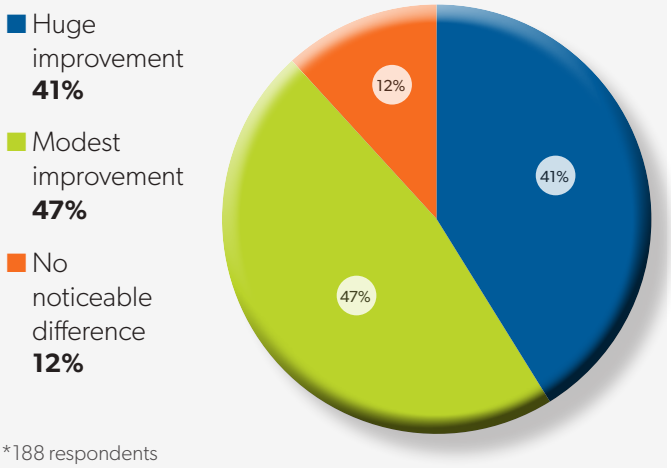
Perhaps mindful of the potential for streamlining costs, twice as many respondents agreed that the "total cost of ownership over the system lifecycle is paramount" (36%) as those who thought that "video surveillance is a commodity buy and all about the initial price point" (19%). The trend




Screenshot from Genetec Security Center, which integrates with IDIS IP cameras

was less pronounced, at 31% and 23% respectively, for owners of plug-and-play systems (figures being 38% and 16% for other systems).

## How much has video analytics improved your security operation?*




*188 respondents

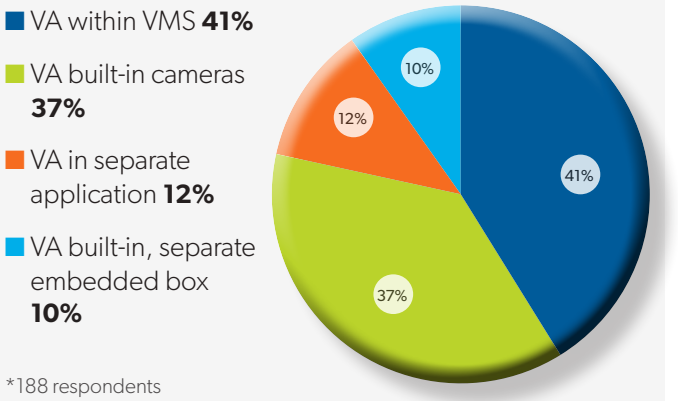
### Analytics on the edge

Hitherto the sole preserve of large corporate or government systems, CCTV software is now more affordable and viable for smaller organisations too thanks to the exponential increase in camera and server processing power. More than half (58%) of respondents have used video analytics, with the vast majority (88%) reporting an improvement in operations as a consequence, with 41% observing a "huge improvement".

This democratisation of access widened further still with the advent of analytics on the 'edge'. Locating the software within the camera itself rather than on the VMS, it reduces the number of servers required and therefore operating costs. Edge-based systems are now only marginally behind VMS-based solutions in terms of prevalence (37% compared to 41%). Filter the data to systems installed in the last five years and video analytics on the edge leads 43% to 37% (against 20% and 52% respectively for older systems).

The most popular function is, as might be expected, the simplest: intrusion detection, which is deployed in 81% of installed systems with analytics. But surveillance software offers growing numbers of functions as standard, with

## What type of video analytics platform do you use?*




*188 respondents

the other main functions in use by 52% (access control applications), 48% (data analysis apps like heatmaps, people counting) and 31% (others: crowd detection, fire/smoke detection).

> **"Video analytics is getting mature and will prove its strength after much upgradation in various areas within the VMS." India-based senior executive**

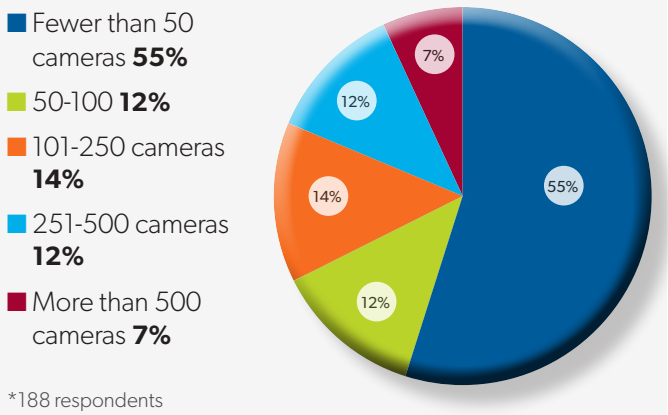
There is still much room for improvement, according to some respondents. One, presumably employed in the shipping industry, said they only used analytics for their 'man overboard' system, but that "at sea, conditions make it still unreliable". The platform can only automate so much, so they still rely on a "proactive CCTV control room. VA technology, while nice to have, is not really necessary in our industry." Another security professional, in the financial sector, said they were "yet to see true value of analytics in the banking industry. We have such a big issue with fraud/card skimming at our ATMs and no CCTV supplier is truly addressing this issue." A UK-based security guard said simply that they were "not terribly impressed with our set-up." Another respondent was scathing of the concept as a whole: "Struggling to see the point in analytical software. Seems to be an 'over the top' buy."

## Which of the following functions does your video analytics system have?

## View from the vendor

"At IDIS we believe that customers shouldn't have to sacrifice quality and functionality for lower prices. However, the price points for many analytics applications put them out of the reach of many smaller businesses and retailers with hundreds of stores. As a result, IDIS launched VA in the Box, a simple plug-and-play device that is perfectly suited to retailers and pitched at an incredibly attractive price point. It gives them access to all the information needed to make them more competitive and to make the best decisions possible." **Brian Song**, *managing director, IDIS Europe*

## How many operational cameras does your analytics system involve?*

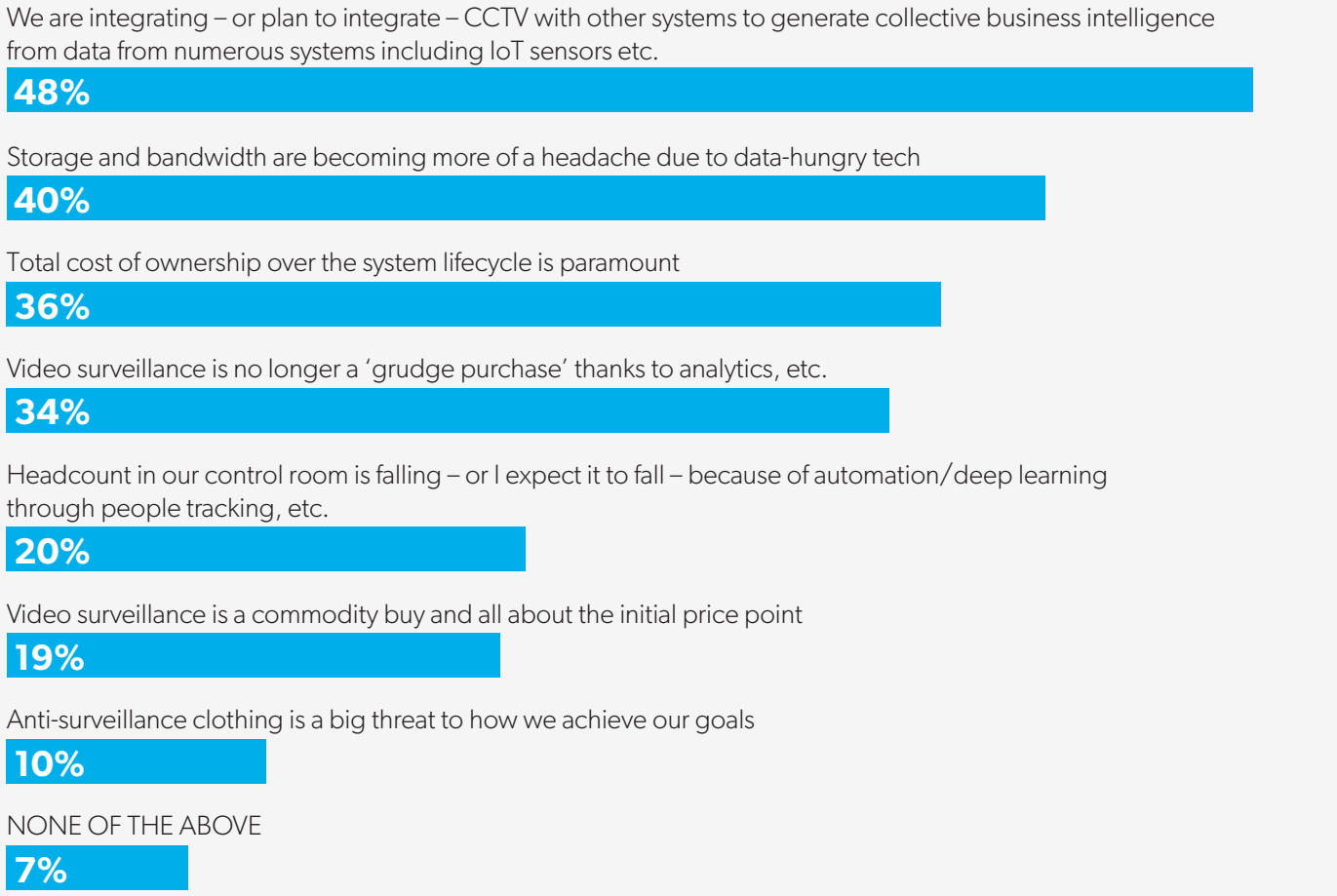



*188 respondents

### Storage challenges

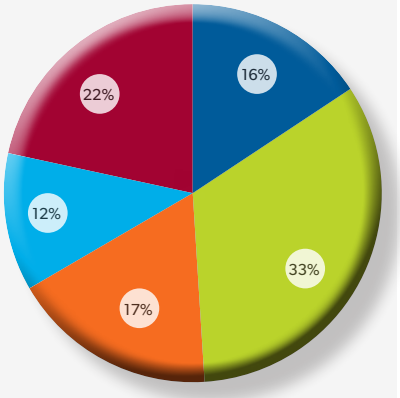
Storage capacity for surveillance systems is soaring because of HD and 4K cameras, full frame rate recording, 24/7 recording, video analytics and growing retention times, among other factors. That two in five (40%) respondents agreed that "storage and bandwidth are becoming more of a headache" is notable not because the proportion is so large, but because we might have expected it to be even higher (interestingly, far fewer respondents with plug-and-play systems, at 31% – versus 44% of those with other systems – agreed with this assertion). Using a cyclic, sequential system, CCTV storage differs from mostly database-driven IT data, which undergoes many read-modify-rewrite processes. Because video data is used as evidence, it is never modified, posing a different set of challenges.

## Which of these statements do you agree with?



## What is the accuracy level of your installed video analytics?*

- 90% or higher **16%**
- 80-89% **33%**
- 70-79% **17%**
- 60-69% **12%**
- Not sure **22%**




*188 respondents

**Innovations like file compression technologies, sequential storage and even the use of helium are helping the industry meet ballooning storage demands**

Nevertheless, innovations like file compression technologies, sequential storage and even the use of helium (whose molecules are smaller than air molecules, reducing friction and vibration and therefore boosting storage capacity) are helping the industry meet ballooning storage demands. Broadband speeds are also rising all the time.

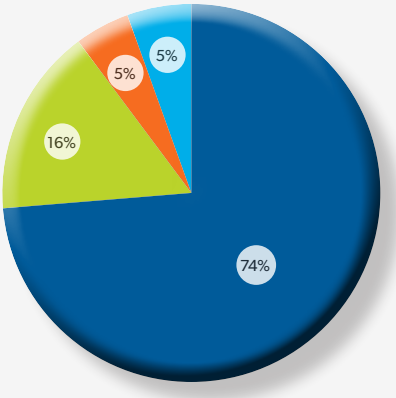
## View from the vendor

"Responding to soaring bandwidth and storage requirements, particularly since the advent of 4K cameras, IDIS announced the development of Intelligent Codec last year. Intelligent Codec is advanced compression technology that dramatically enhances IDIS's complete H.265 range of full-HD IP cameras and network video recorders (NVRs), which already deliver up to 50% bit rate reduction savings on storage space and network bandwidth. IDIS Intelligent Codec delivers up to 30% bit rate reduction on top of H.265, achieving a total 65% reduction for users. Leveraging IDIS motion adaptive transmission (MAT) technology – which reduces bit-rate by restricting transmission during live surveillance periods without movement – IDIS delivers a further reduction. From an H.264 baseline, IDIS Intelligent Codec plus MAT delivers total savings of up to 90%, depending on scene and resolution. The less complex the scene and the less movement present, the greater the compression." **Brian Song**, *managing director, IDIS Europe*

# 5. Warranties

## When was your current video surveillance system installed?*

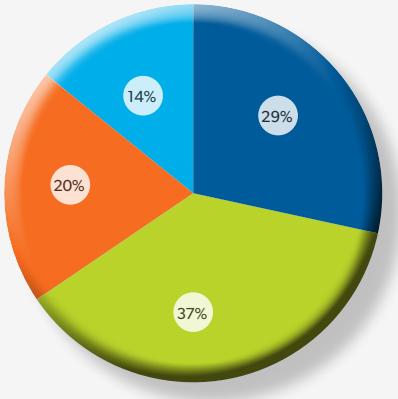
- In the last 5 years **74%**
- 6-10 years ago **16%**
- 11-15 years ago **5%**
- More than 15 years ago **5%**




*241 respondents

## How often do you replace your surveillance system?*

- Less than every 5 years **29%**
- Every 5-7 years **37%**
- Every 8-10 years **20%**
- More than than every 10 years **14%**




*202 respondents

More than a third of organisations replace or upgrade their CCTV systems every 5-7 years and the median average sits within this band. The median product lifespan, as estimated by our respondents, is in a similar ballpark, at 4-6 years, for both cameras and recorders. Organisations are therefore seemingly, by and large, replacing or upgrading systems as they approach the end of their useful life.

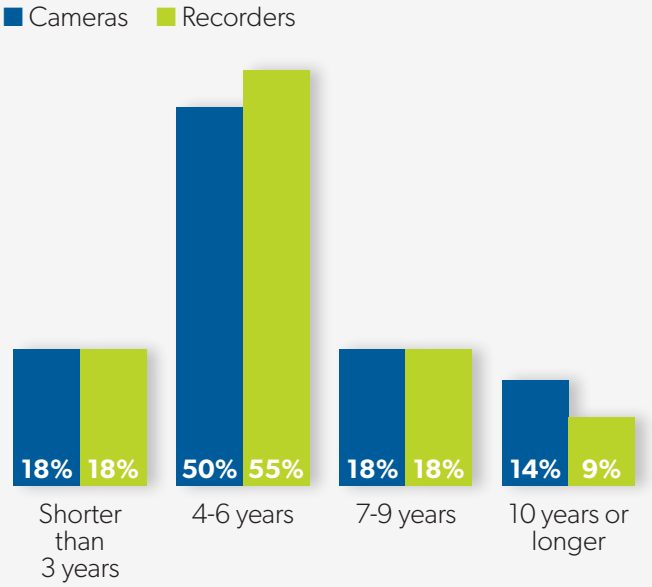
But what might prompt security professionals to conclude that a system has reached the end of its useful lifespan? There are three obvious scenarios. One, the cost of running and maintaining the system becomes too prohibitive to justify commercially. Two, replacement parts are no longer available or the vendor no longer supports software updates. Or three, the performance and functionality of a

## View from the vendor

"IDIS designs, develops and manufactures everything in-house with quality and reliability in mind, adhering to various certifications including Six Sigma, which simply means a measure of quality that strives for near perfection and must not produce more than 3.4 defects per million products. Many of our customers such as the Dutch postal service, PostNL, will testify to still having our DVRs still in operation with little to no maintenance in over 13 years – a clear demonstration of the IDIS signature of quality and reliability." **Brian Song**, *managing director, IDIS Europe*

legacy system is so inferior to that of the latest generation of surveillance technology that the system can no longer be reasonably described as fit for purpose.

## What lifespan do you expect from the following products?

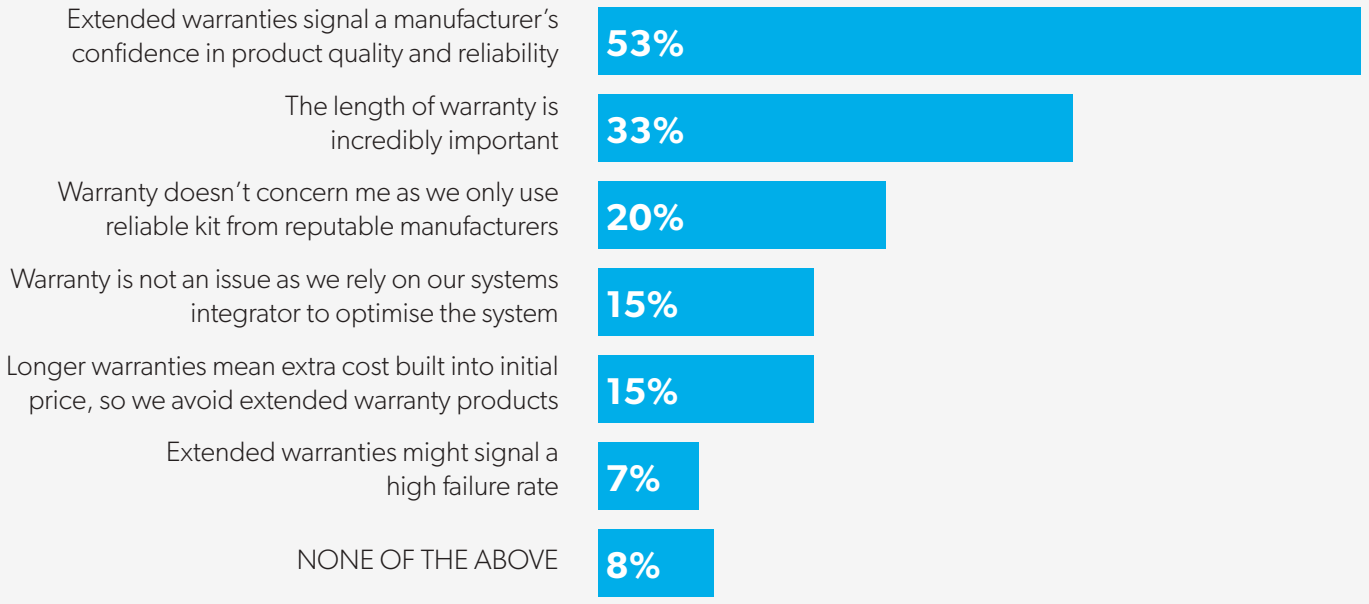



Asked about the importance of warranty when considering upgrading or procuring a surveillance system, one in three (33%) of those polled agreed that "the length of warranty is incredibly important". But for one respondent, the terms and duration of the warranty itself was less significant than the integrity of the person providing it. "The length of a warranty should be measured against an installer's, integrator's, consultant's, distributor's or manufacturer's willingness to honour the warranty," they wrote. "Too many companies offer longer term warranties, but at the moment of truth they decline to take responsibility and will blame anything that comes to mind to ensure that they are not responsible."

Only one in five (20%) asserted that the "warranty doesn't concern me as we only use reputable kit from manufacturers that have proven reliable" – a clear signal to the industry that warranties matter, regardless of brand reputation.

> **"For me, longer warranties signal a manufacturer's confidence in their system." UK-based senior security professional**

## Which of these statements do you agree with about the importance of warranty when you consider upgrading/procuring a surveillance system?



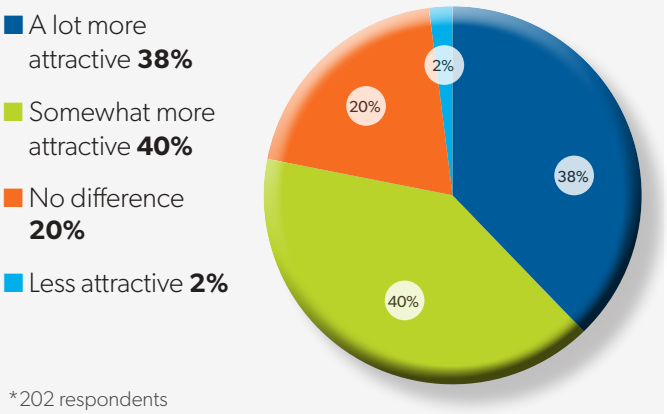
But the aforementioned respondent, who was among that 20%, insists that a warranty can never compensate for misgivings over quality. "A three- or five-year warranty [is little different to] a one- or two-year warranty if no one is actually going to honour it. Stick to a mainstream brand where you have leverage and they will honour what they say," they recommend.

Another respondent was sceptical about the concept of warranties full stop – in any industry. "As with domestic equipment, the electronics are designed to fail after a certain time – if they didn't, the manufacturers wouldn't make a profit," they wrote. "Warranties will always have enough wriggle room to make them nothing more than window dressing" – and that comment was from an electronics engineer.

The industry was split almost down the middle as to whether extended warranties signal that a manufacturer is confident of product quality and reliability. Yet there was a clear consensus about the converse proposition; 93% disagreed with the notion that "extended warranties might signal a high failure rate". And 85% dissented from the view that "longer warranties mean extra cost built into the initial price point." All in all, then, most security professionals are not at all suspicious of extended warranties and more than half (54%) even think they represent a kind of unofficial seal of quality. While a not inconsiderable total of 45% ticked at least one statement that questions the value of warranties, 65% ticked one or both statements extolling their benefits.

Moreover, the offer of a five-year warranty without additional cost (most vendors offer only three) would make a surveillance solution a more attractive proposition to nearly four in five (78%). Given that 78% and 73% respectively think the lifespan of cameras and recorders are six years or less – and 17% and 18% think they are shorter than three years – this is perhaps understandable.

**Most manufacturers offer 3-year warranty. How much more attractive would a manufacturer offering 5-year warranty be without any additional cost?***




*202 respondents

A security professional based in Nigeria said that most warranties in the country "last for just one year, so the onus is really on products to maintain their brand quality and integrity." There is also an onus on technology buyers to do their due diligence before committing, according to another respondent: "Total cost of ownership is impacted by licences, upgrades and hidden high cost of support and maintenance. It is important to define and agree on present and future costs through a comprehensive (SLA) [service level agreement] contract with the supplier at purchase and before installation of equipment."