NW Security Group

Preparing for the Next Generation of CCTV Systems

Report of findings amongst senior managers responsible for running CCTV systems across businesses in England

March 2021

Background to the study

During September 2020, NW Security Group commissioned an in-depth study of businesses with more than 50 employees which are running their own CCTV systems. We wanted to explore the plans that medium and large-sized businesses had for their existing CCTV systems right across England.

Areas of specific focus for the study included ‘Cloud CCTV’ adoption as new Video Surveillance as a Service (VSaaS) offerings begin to fill out and gain market traction.

We also wanted to explore whether COVID-19 was accelerating Cloud CCTV migration plans. We wanted to probe how advanced businesses’ plans were for the redeployment of existing network video systems to help keep workspaces safe for staff that needed to carry on working on site right through the pandemic.

We have also been able to explore the extent of companies’ increasing appetite for remote monitoring of operations now that so many security chiefs, IT heads and facilities management teams are spending so much time working from home.

Because we have been focused on the network video world for nearly 20 years, it is always important for NW Security to track the extent of the switch to network video from traditional analogue-based CCTV systems. We found that the elusive CCTV to Network Video tipping point has finally been reached.

Just over half of England-based large businesses with over 250 employees have switched to network video, while just over two-thirds of medium-sized businesses with 50 to 250 employees have already migrated CCTV systems onto the network.

56%

Large businesses in England have switched to network video

69%

Medium businesses in England have migrated CCTV onto the network

We also asked several questions to probe how firms were managing their CCTV systems today. We looked for the extent of penetration of outsourced professional security services and expertise.

We went deeper still to ask whether those in charge of CCTV systems were happy with the quality and return on investment they were generating from their systems. We spotted a good deal of disquiet amongst managers of CCTV systems in our research findings in this area and have dedicated a whole chapter to these findings.

Closer to home for NW Security, we asked businesses running CCTV system which services and capabilities they were most likely to search out. For example, we queried the importance of cloud migration skills for those looking for security integrators and consultants to support them looking forward.

We also used this study to begin to track the types of businesses which were most likely to want to purchase CCTV support services via a managed security service paid for through a monthly usage-based subscription, thus paying for CCTV systems management out of OPEX rather than CAPEX.

A good many of the findings confirmed what our existing customers and prospects have been telling us. However, this report also reveals some genuine surprises which we hope you will find as interesting and enlightening as we did.

Happy reading!

Frank Crouwel

Managing Director

NW Security Group

NW Security Group

Contents

1 – Setting the scene

NW Security Group decided to commission this study to confirm what it anticipated from discussions with prospects and existing customers; that businesses running CCTV systems are increasingly struggling with optimising their systems using in-house resources alone.

A combination of the adoption of second-generation AI-led video analytics capabilities, the move to network video technologies and the potential offered by Cloud CCTV is creating anxiety amongst CCTV system users. This study probes the extent of that anxiety and what it means for integrators which can help firms navigate a sea of changes, undoubtedly accelerated by the pandemic.

Nationally-respected market research firm Opinium, executed this survey which was completed by 101 IT decision makers of England-based firms with more than 50 employees between 8th and 14th September 2020. Only firms with CCTV systems were invited to complete the survey.

Respondents were weighted towards senior IT Decision Makers: 29% were IT Managers, 33% IT Directors, 10% CTOs, 8% CIOs and 7% Operations Directors. The balance were Operations Managers or equivalent.

Which job title most accurately describes your primary role?

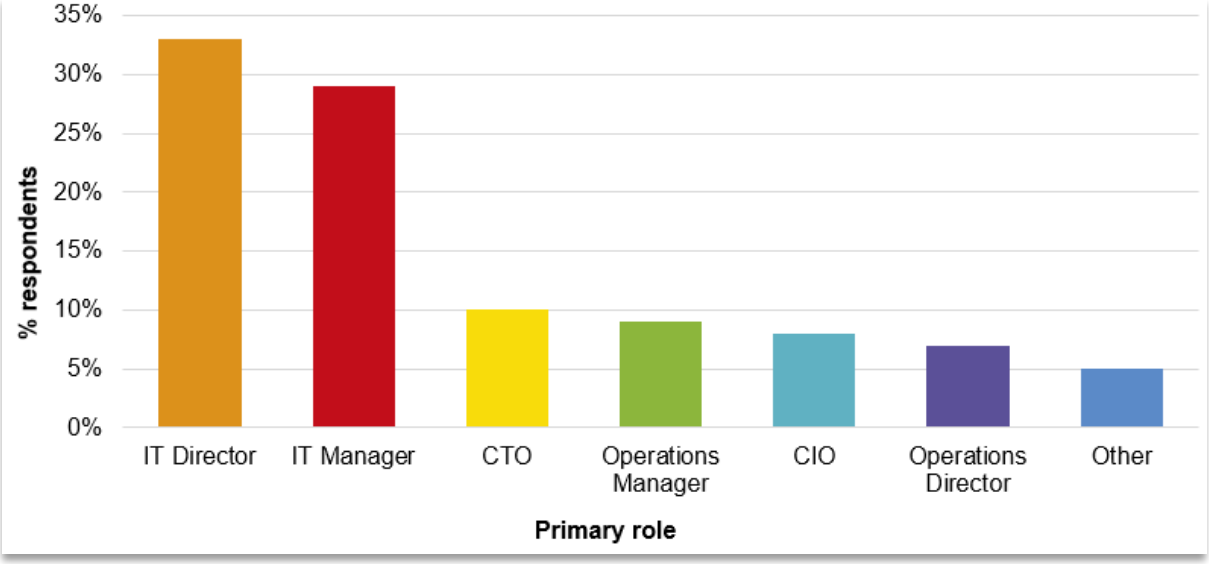


Figure 1: Breakdown of respondents within England-based businesses with over 50 employees which had their own CCTV systems.

2 – CCTV cloud migration trends

One key revelation from the comprehensive study which NW Security commissioned in September 2020 was many businesses' level of conviction around plans to migrate existing CCTV Systems into the cloud. This was especially surprising given the complexities associated with running CCTV from the cloud, when compared with traditional IT services such as email, CRM and ERP systems which have been the first in line for 'putting into the cloud'.

Two thirds of private sector-run CCTV systems set for cloud migration

The private sector is leading the charge, our study discovered. Over two thirds (71%) of medium and large-sized firms in the private sector are planning to migrate their existing systems into the cloud within the next 12 months i.e. by September 2021. By comparison, less than half of public sector organisations (43%) are planning to move their CCTV systems into the cloud within the same timeframe.

An average of 58% of all public and private sector businesses captured in this England-wide survey are planning to migrate their existing CCTV systems into the cloud over the next 12 months.

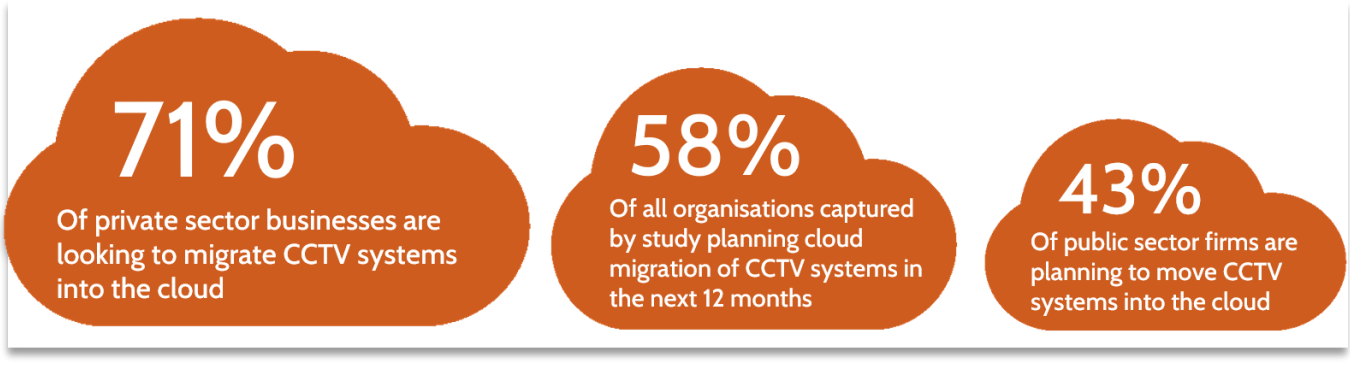


Figure 2: Over half of all CCTV system owners are planning to migrate their systems into the cloud by September 2021.

Construction sector is early adopter

The most significant early adopter sector for 'Cloud CCTV' is construction, where 89% of medium-sized firms (with 50 to 249 employees) and large firms with 250 or more staff are migrating their video security systems into the cloud over the next 12 months.

The second most enthusiastic Cloud CCTV adopter is the wholesale distribution and retail sector, where 80% are planning CCTV system migration into the cloud.

The third fastest Cloud CCTV adopters are manufacturers, with 78% of respondents to our survey migrating, or planning CCTV system migration, into the cloud over the next 12 months.

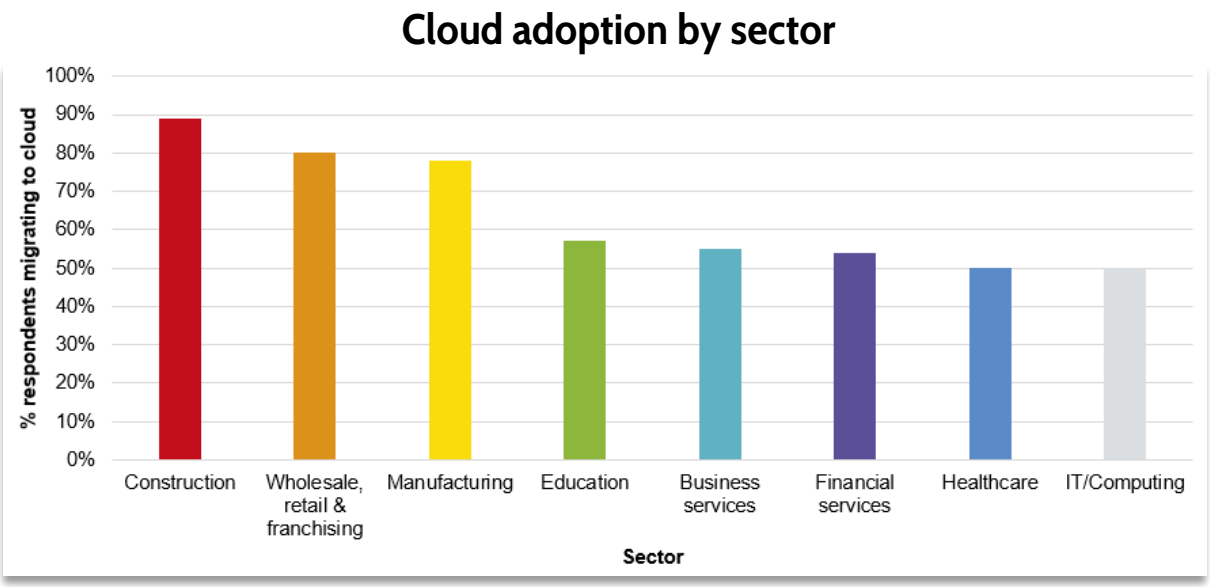


Figure 3: Cloud adoption sector hotspots.

CCTV vs. Network video 'tipping point' reached across all sectors

61% of England-based medium and large businesses had network video monitoring systems rather than traditional analogue-based CCTV systems, the new study found.

It took over 20 years from the invention of the world's first network camera by Axis Communications in 1996 for us to reach this important market milestone here in the UK.

Why so long for the tipping point to be reached here? The reason is likely to be that the UK was an enthusiastic early adopter of

traditional analogue-based CCTV in the 1970s and 1980s. Heavy deployment by the mid-1980s meant that when more sophisticated network video systems arrived, few councils, police forces and other system users were prepared to invest in ripping out CCTV infrastructure which was still serviceable.

This slowed adoption of network cameras and network video equipment where much of the innovation was taking place from the late 90s. Use of legacy systems was perpetuated by innovation in analogue to IP video transmission equipment which extended the life of many CCTV cameras and CCTV infrastructure, particularly in the public sector.

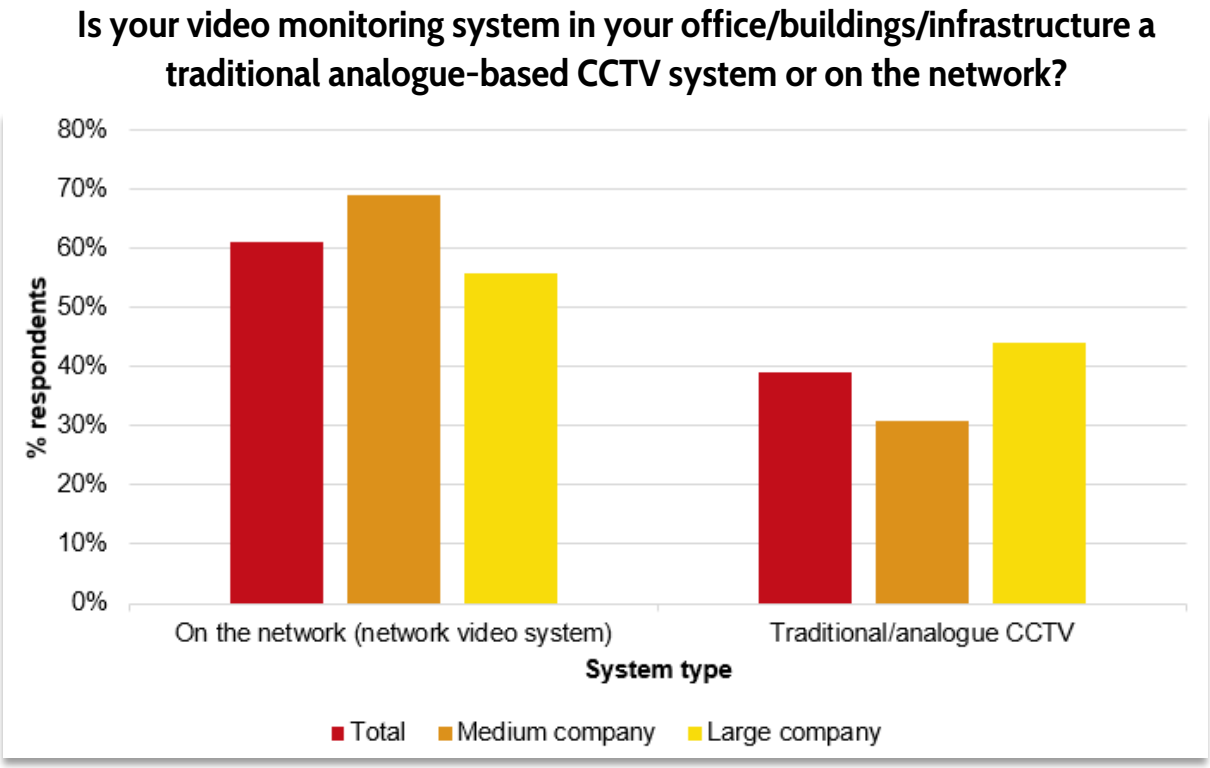


Figure 4: More than two thirds of medium-sized businesses in England now run their CCTV systems on an IP network.

However, now that significantly more systems are networked and remaining CCTV infrastructure is reaching end of life, the UK has become a hot spot for migration of systems onto the network. Once on the network, it is of course much easier to move them into the cloud – and the technology is ready. A number of Video Surveillance as a Service (VSaaS) offerings are now available and Cloud CCTV services are reaching the UK market just as Cloud CCTV demand is growing.

Cloud adoption accelerated by COVID-19

Cloud CCTV fits into wider cloud migration plans which have been accelerated in response to COVID-19. 42% of all medium and large-sized businesses admitted that their '*cloud migration plans are being accelerated in 2020/21 because of COVID-19*'. A further 34% increased budgets to put more IT services and applications into the cloud following the outbreak of the pandemic.

Three quarters (78%) of firms which completed NW Security's business survey carried out during September 2020 across England, confirmed that they had accelerated cloud migration plans as a result of the pandemic.

Has COVID-19 impacted the speed of migrating applications into the cloud?

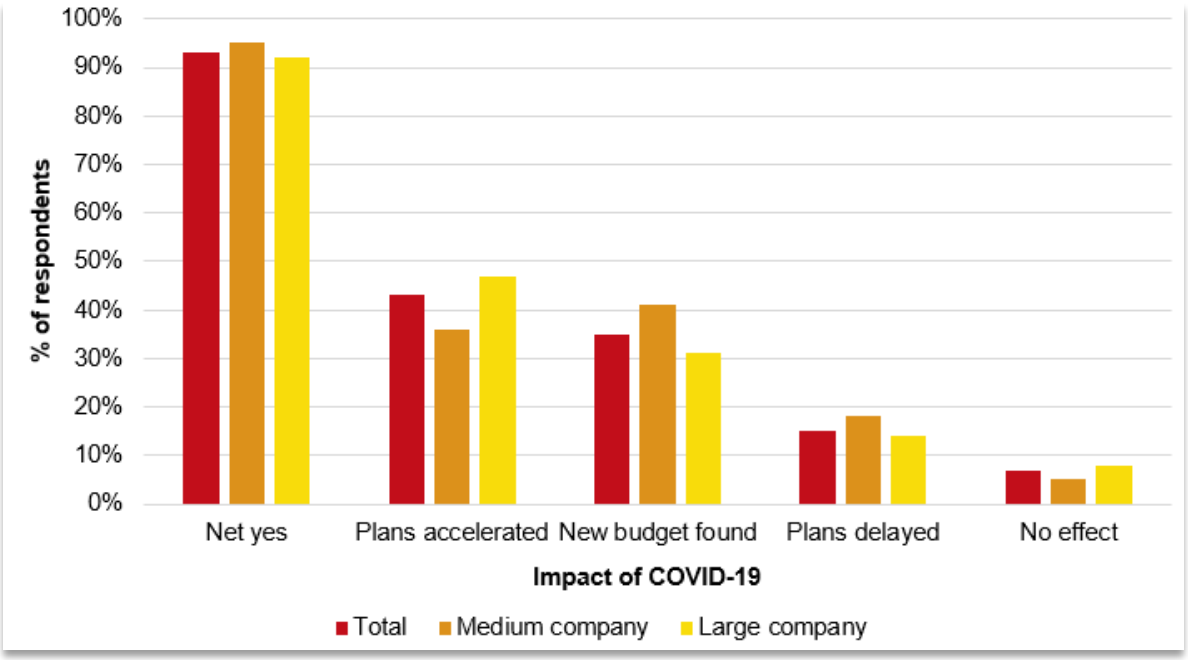


Figure 5: Nearly half of large businesses are accelerating their cloud migration plans because of COVID-19.

Cyber security budgets increasing

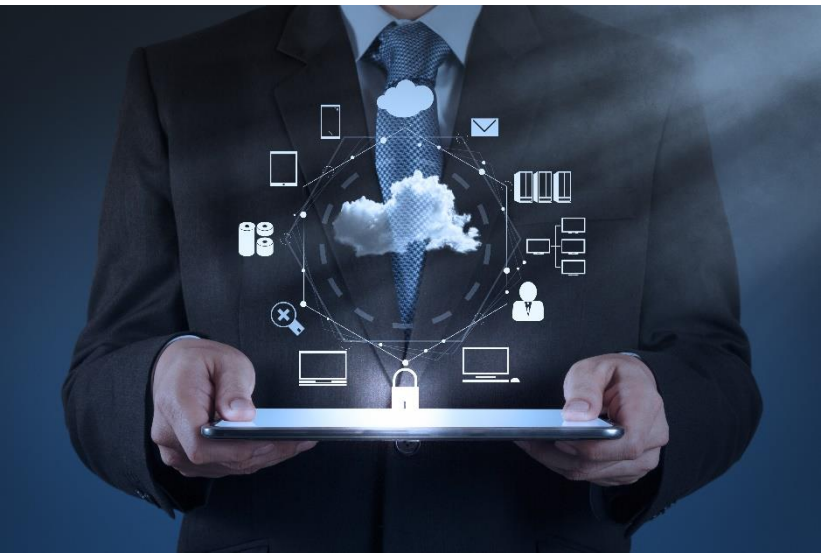
In terms of other irreversible security technology trends which medium and large-sized businesses predicted; there were three 'stand out' sectors which foresaw a tighter focus on cyber security across all networked systems as an irreversible IT change precipitated by COVID-19. 50% of healthcare operations, 46% of financial services firms and 43% of schools and colleges flagged the rise of cyber security concerns and corresponding budgets to harden systems.

OPEX rather than CAPEX IT 'servitization' trend driving cloud adoption

Cloud migration tends to be favoured by firms facing pressures to reduce Capital Expenditure (CAPEX) in favour of purchasing and running IT applications via subscription services out of ongoing Operational Expenditure, or OPEX.

1 in every 6 (16%) private sector firms in this study saw '*increased scrutiny of costs and a move from CAPEX to OPEX spending*' as a trend that was being irreversibly accelerated by COVID-19.

The professional services sector were the most enthusiastic adopters of this way of thinking – a third (33%) of them saw OPEX rather than CAPEX as an irreversible governor of IT decision-making following the pandemic.



"In short, there's a greater appetite to move more applications into the cloud and CCTV is finally part of that acceleration."

Frank Crouwel, Managing Director of NW Security Group

5 key drivers of cloud migration

There are five key reasons for the accelerating cloud migration that our study of CCTV system owners found

1. 'Remote Everything'

COVID-19 is stimulating an acceleration in the migration of all IT applications into the cloud, creating a 'Remote Everything' phenomenon, as we like to call it. It makes sense, with so many of us working away from our normal workplaces, that remote access to all essential systems is enabled. For many, that's naturally led to a push to put more systems into the cloud.

Early adopter cloud-based system users recommend it over accessing on-premise systems remotely because of the ease of access and retrieval of data. 'Cloud first' solutions claim to come with improved resilience, tighter cyber security, and easier system management for IT managers.

2. CCTV to network video tipping point

The UK has finally gone through its 'CCTV to Network Video' tipping point, so that 61% of all UK-installed CCTV systems are now on an IP network. As such, many more video management systems are that much easier to migrate into the cloud now they are on the network.

3. 'Servitization' of IT systems

You also need to set cloud migration in the context of a wider drive to 'servitize' IT systems to accommodate IT decision-makers and C-suite executives who want to pay for all network-based services based on usage levels, rather like a utility.

Servitization fuels cloud migration as this is the preferred way of delivering IT services via affordable monthly subscriptions, while delivering highly reliable, highly scalable IT services with near 100% uptime.

4. A desire for remote management

Cloud migration supports a growing trend for managers to request access to video evidence wherever they are. Why? Network camera data is increasingly being used to check site operations, as well as ensuring security of premises and the health and safety of workers – all remotely.

Video data is attracting more remote managers as video analytics wizardry offers the capability to deliver new insights

linked to the inner workings of a business. It is part of the phenomenon that we call Remote Everything - more on that later.

5. Efficiency and cost-effectiveness

Not having to maintain a dedicated server, with video management software licenses, in the cramped backroom of each and every premises you run is appealing. The hardware cost savings and ongoing management efficiencies alone are obvious when you multiply that by the number of sites you run.

With Cloud CCTV, cameras can be connected directly to the internet and no other equipment is needed, whilst users experience the systems remotely through standard web-browsers and smart mobile apps like many other cloud-based services.

Tipping Point Reached

61%

Of all UK-installed CCTV systems are now on an IP network, making it that much easier for users to migrate these systems into the cloud

Remote Everything re-energised

In all this, it's worth looking at the growing trend which we like to call Remote Everything. When we started NW Security back in 2004, with IP video technology at its heart, we had a vision to not only deliver relevant video data to the right people at the right time, but also to use this technology to significantly reduce unnecessary travel time, saving money and, importantly, reducing environmental impact.

However, our Remote Everything vision was only slowly and partially realised - until now at least. The COVID-19 pandemic is making Remote Everything more inevitable. Working from home or away from the workplace (and the consequent reduction of business travel) has become common globally.

Many predict this phenomenon is here to stay even after COVID-19 recedes. The need to travel for business has become scrutinised at many levels. We are all finding new ways and remote online tools to do our work without leaving our homes if necessary.

Good planning essential

Although there are many drivers at work making cloud CCTV adoption inevitable; we are sounding a note of caution having worked with several companies preparing to make these moves.

Use this planning as an opportunity to review and restate your Standard Operating Procedures (SOP) and requirements for your system. Failing to do so may eliminate anticipated savings from moving your system into the cloud.

The COVID-19 pandemic is making Remote Everything more inevitable – working at home has become common globally and many predict the phenomenon is here to stay

Video retention and playback review

You must consider that managing video data is not as simple as typical data flowing through corporate computer networks. Video data transmission requires much more bandwidth and storage resources. Large volumes of data can be accumulated quickly. Much of it may never be accessed, unlike typical business files. We recommend a thorough assessment of data being accumulated as well as your retention and deletion regimes.

You need to work out what frame rates are needed as well as anticipated playback usage and speed of access when required. It will vary according to the location of each camera. Without doing this preparation work, migrating to the cloud could actually end up costing you more.

Legacy CCTV system recording retention regimes as long as 30 days - which are still common in public space centralised monitoring units - must be reviewed if cloud migration is being planned.

A thorough review of SOPs often uncovers a finding that CCTV recordings older than 7 days are rarely, if ever, requested. Normally security incidents are reported within 72 hours of occurrence. Asking the right questions and probing actual and required usage can lead to as much as a 75% reduction of video storage – very significant savings when you are paying by the Mega Byte for readily-available cloud storage.

Data costs money – it's important to carefully consider how much data needs to be stored, and for how long, according to real operational needs

IaaS Vs VSaaS

IaaS provides less restricted features and functionality; but requires much more hands-on maintenance than more restrictive VSaaS

IaaS versus VSaaS decision

Can the VSaaS service you are considering handle CPU-hungry video analytics which have been increasingly deployed in on-premise servers? Only basic video analytics capabilities are currently available from VSaaS providers today.

If you are looking to use more advanced video analytics available inside the latest cameras 'on the edge' then moving your existing Video Management Software (VMS) into an Infrastructure as a Service (IaaS) platform like AWS or Google Cloud would be a more suitable option to avoid losing functionality you may be reliant on to capture specific exceptions, for example. Some VMSs have already prepared cloud migration paths with specific IaaS providers. Milestone, for example, has a partnership for this purpose with AWS.

Running your existing VMS in an IaaS environment will give you all the features and functionality that the same software would deliver if you kept it on-premise.

Moving to a VSaaS provider, such as Morphean or Arcules, will restrict you to the features and functionality already available within these platforms. Also be aware that most VSaaS providers have not yet completed the building of their integration partner network. It's likely to take a couple more years for a wide range of integrators with the right skills to be available for your VSaaS of choice.

Cloud fundamentals

It is becoming clearer that moving CCTV systems ‘lock stock and barrel’ up into your IaaS provider of choice is not for the faint-hearted. Those selecting this route may be operating ‘Cloud First’ IT strategies which demand a wholesale migration. However, even Cloud First evangelists should hesitate when considering porting CCTV systems into the cloud. The sheer volume of data generated by all those simultaneous steams of high-resolution video data demands a great deal of bandwidth to move that data and provide high quality playback in microseconds following an incident.

It’s likely to be the most expensive way to migrate CCTV capabilities into the cloud and, as such, will tend to appeal to large enterprises with deep pockets and complex needs. It will be the preserve of businesses which have the internal resources and skills on tap to continue managing their own VMS. It’s also for those demanding full continuity of service post-migration in terms of access to rich feature sets and system configuration.

By contrast, those selecting a VSaaS provider are likely to be organisations which are highly dispersed with not many cameras in each location and very limited access to expertise to fix problems on each of those many sites. It’s perhaps no surprise therefore that one of Arcules’ earliest and largest customers was the co-working spaces provider WeWork.

Retail groups are also amongst the early adopters of VSaaS. For this type of customer, convenience, easy access to recorded images and keeping running costs in line with usage is the key. They are prepared to compromise in terms of the feature sets on offer. They can wait for the latest video analytics capabilities, for example.

The key for those selecting VSaaS providers right now is to get sight of their innovation roadmap. It's also important to be aware that most VSaaS providers are heavily geared and are funded by VCs so there is an inherent fragility to their funding models.

It's important for those selecting a VSaaS provider to establish how much money they are burning each month, when they are projected to move into profit, how many customers they need and how quickly.

This is definitely an area to revisit in a follow-up study that we plan to commission as the VSaaS market matures.

"NW Security intends to conduct follow-up research to track increased penetration of the VSaaS market as feature sets are built out and they begin reaching beyond the innovators and early adopters which normally represent no more than 13% of the overall potential market."

Frank Crouwel

3 – In-house versus outsource: who is managing your CCTV systems?

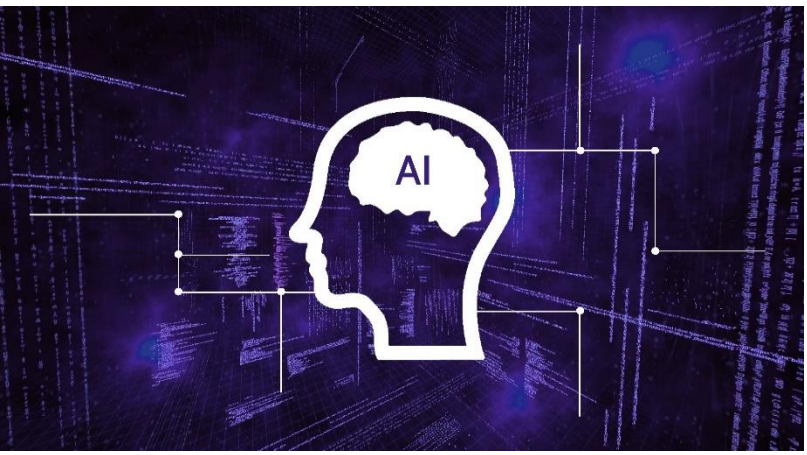
As CCTV systems become increasingly sophisticated, the potential to do more with them increases. Well over half of England's medium and large business CCTV systems are already on an IP network.

In recent years, we've seen object detection and facial recognition solutions being built into security systems, alongside 'first generation' video analytics capabilities such as motion detection and tripwire.

Pauline Norstrom, CEO of AI specialist consultant Anekanta Consulting, explains:

"Automatic and live facial recognition algorithms solve very specific problems of authentication of authorised persons or, indeed, unauthorised persons. Object detection determines the presence of objects and people with defined characteristics such as a car type, whether the individual is an adult or a child and the type of clothing they're wearing. These technologies are analysing the video sources in isolation…. (But) a combination of AI technologies could correlate the outputs of a number of siloed AIs and paint a bigger picture."

In addition to the potential of all this new intelligence being injected into CCTV systems, has come the ability to bring a plethora of security and safety systems together to offer a deeper and more holistic view from which to analyse threats which require further investigation. For example, fire detection, intruder alarms, access control and building management systems can all be brought together and configured to optimise systems.



"A combination of AI technologies could correlate the outputs of a number of siloed AIs and paint a bigger picture."

Pauline Norstrom, CEO of Anekanta Consulting

In the light of all this, IT skills would seem to be increasingly important, particularly in view of businesses' appetite for moving their CCTV systems into the cloud.

33% of CCTV systems are managed by security or FM teams

Despite the technology trends outlined above, facilities management (FM) and security departments still manage a third (33%) of all medium and large-sized businesses' CCTV systems today. This is not necessarily bad news though, as it creates an opportunity to access discrete skills and expertise by identifying the right specialist integrators and consultants.

Frank Crouwel, Managing Director of NW Security, commented:

"For me, it represents a big opportunity for specialist security integrators like NW Security to assist in-house teams in updating and optimising their existing systems as the technology has improved significantly in recent years, making it much more difficult for in-house teams to keep systems optimised."

> "Many IT managers are being forced to take a deeper interest now that the technology and installer partner capability is available to upgrade and improve CCTV systems, potentially moving them up into the cloud and exploring the application of new AI-driven video analytics capabilities."
>
> Frank Crouwel

27% of CCTV systems are managed by IT

That said, IT departments are finally catching up: just over a quarter (27%) of CCTV systems are now managed by IT departments, our study found.

As more CCTV systems depend on the IT and cyber security skills of the IT department to keep them running - especially as more systems are migrated into the cloud - it becomes inevitable that more CCTV systems will be managed, maintained, configured, and upgraded within companies' IT departments; perhaps working in collaboration with their security or facilities management teams.

Only 29% fully outsourced CCTV management

Despite the increased complexity of CCTV surveillance systems, only 29% of firms with over 50 employees have outsourced the management of their CCTV systems to an external security company.

Public sector bodies are slightly more likely to outsource security management: 31% of public sector respondents had fully outsourced security systems support and management.

Many firms have already included CCTV system maintenance and management within their centralised and unified ICT (information communication technology) service provision.

By bringing all parts of ICT together, concentrating the network and IT infrastructure skills in one place, you can ensure the IP video monitoring system gets the attention it deserves to timetable relevant software and firmware updates as well as camera optimisation work.

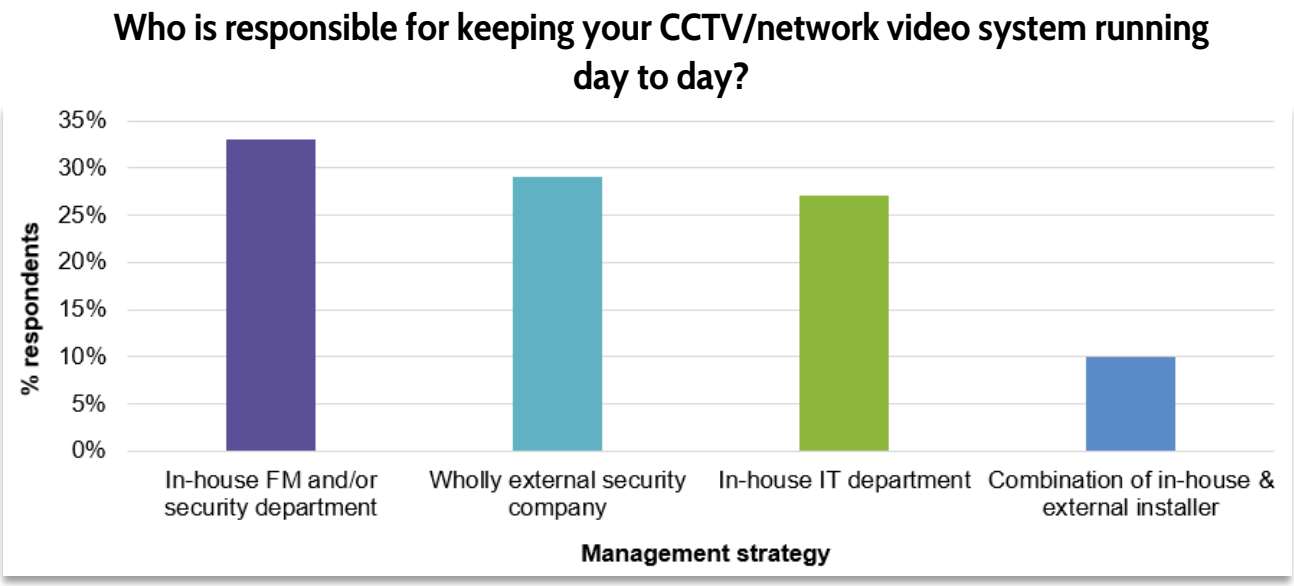


Figure 6: 60% of all firms still manage their CCTV systems in-house between their FM, Security and IT departments.

It also needs to be acknowledged that network video is a specialist field. It's experiencing rapid technological and market change which can only be tracked and managed if sufficient resource is put in place.

However, NW Security's experience confirms that only the largest businesses, those with over 250 employees, tend to have sufficient capacity within their ICT, FM and/or security teams to keep permanently up to speed with IP video systems.

4 – Value in strong partnerships

A quarter of firms also planned to select a partner based on evidence of '*strong partnerships with best of breed vendors and service providers*.' Nearly a third (32%) would select based on a third-party installers' '*collaborative approach to working with us to improve our CCTV system and how it is supported*'.

NW Security believes the need to collaborate effectively both between key in-house departments including FM, IT, and security functions, and with outside expert installers, integrators, and consultants, has never been more important.

No one department is likely to have the monopoly on knowledge now that more than half of CCTV systems have been ported onto an IP network; the next generation of AI-driven video analytics is arriving; and cloud migration of CCTV systems is becoming increasingly viable and attractive.

Medium-sized firms more open to collaboration with external experts

Medium-sized firms with 50-249 employees captured by this study tend to struggle to keep IP video systems working optimally over long periods of time without external specialist help.

Frank Crouwel explains:

"Understandably, we have much more experience of working with these sorts of businesses. When we get to a site managed by one of these organisations, we often find some cameras not working at all; others might need cleaning or rewiring. Sometimes new threats have emerged which demand installation of new or more modern, higher spec cameras. There is new regulation like GDPR to comply with.

"If there is a great deal of work to do, it's common for us to work in tandem with ICT or Facilities Management staff to source, install, configure and network different equipment.

> **"The key is to work with the skills and resources companies already have on tap."**
>
> **Frank Crouwel**

"So, an engineering company might be very able to source and install a CCTV-ready mast for providing coverage of a fenced in yard which holds high value stock for example. However, we might install the right cameras for that mast, and then configure and network it. It's important to be open to sharing out the work to keep upgrade and maintenance costs to a minimum, while not compromising on quality and effectiveness."

Hybrid partnership approach set to gain ground

1 in 10 medium and large-sized businesses (10%) have adopted a hybrid approach: working with a security installer for their expertise when needed, whilst still managing their CCTV systems day-to-day in-house.

Frank Crouwel again:

"We are seeing more businesses looking for help from expert partners for upgrade, improvement and optimisation of CCTV systems to ensure they are getting optimal value from their existing systems.

"So, I was a bit surprised to find that only 1 in every 10 firms captured by our study had a declared policy of working with an external partner today. This finding is worthy of further investigation during 2021. I suspect more will outsource to trusted experts as systems become more feature rich and Cloud CCTV migration levels rise."

NW Security believes that the CCTV market is undergoing fundamental change and plans to investigate the implications of that change in a second study that it will run this year. This first study, conducted in September 2020, indicated businesses were starting to expect more from both their systems and from the installers and contractors that support them.

There was also early evidence that, as companies consider moving CCTV systems up into the cloud, they are tending to in-source more CCTV management decision-making as they focus on upskilling internally. These changes will be explored in NW Security's 2021 market study.

"We are seeing more businesses looking for help from expert partners for the upgrading, improvement and optimisation of CCTV systems."

Frank Crouwel

Around the clock 'Emergency Service' support vital for CCTV users

When asked what criteria directors or senior management in charge of CCTV systems would use if they needed to select a new security systems installer, the top criterion for selection was '*access to Emergency Service support around the clock.*' 43% of firms with an existing CCTV system would select based on availability of a full out of hours emergency service in case of incidents.

Nearly as many, 38%, would select based on '*evidence of CCTV and network video monitoring capability and pedigree*'.

Cloud capability increasingly important in partner selection

However, so called 'Cloud CCTV' capability is also becoming a major factor in the selection of any security installation partner.

NW Security's study found nearly a third (32%) of firms would seek "*evidence of cloud migration and 'in the cloud' CCTV management capability*" when selecting a security installer.

This is perhaps no great surprise when the same study also found over two thirds (71%) of private sector firms are planning to migrate their existing CCTV systems into the cloud within the next 12 months.

What are the main things you would look for in a CCTV/security system installer/provider?

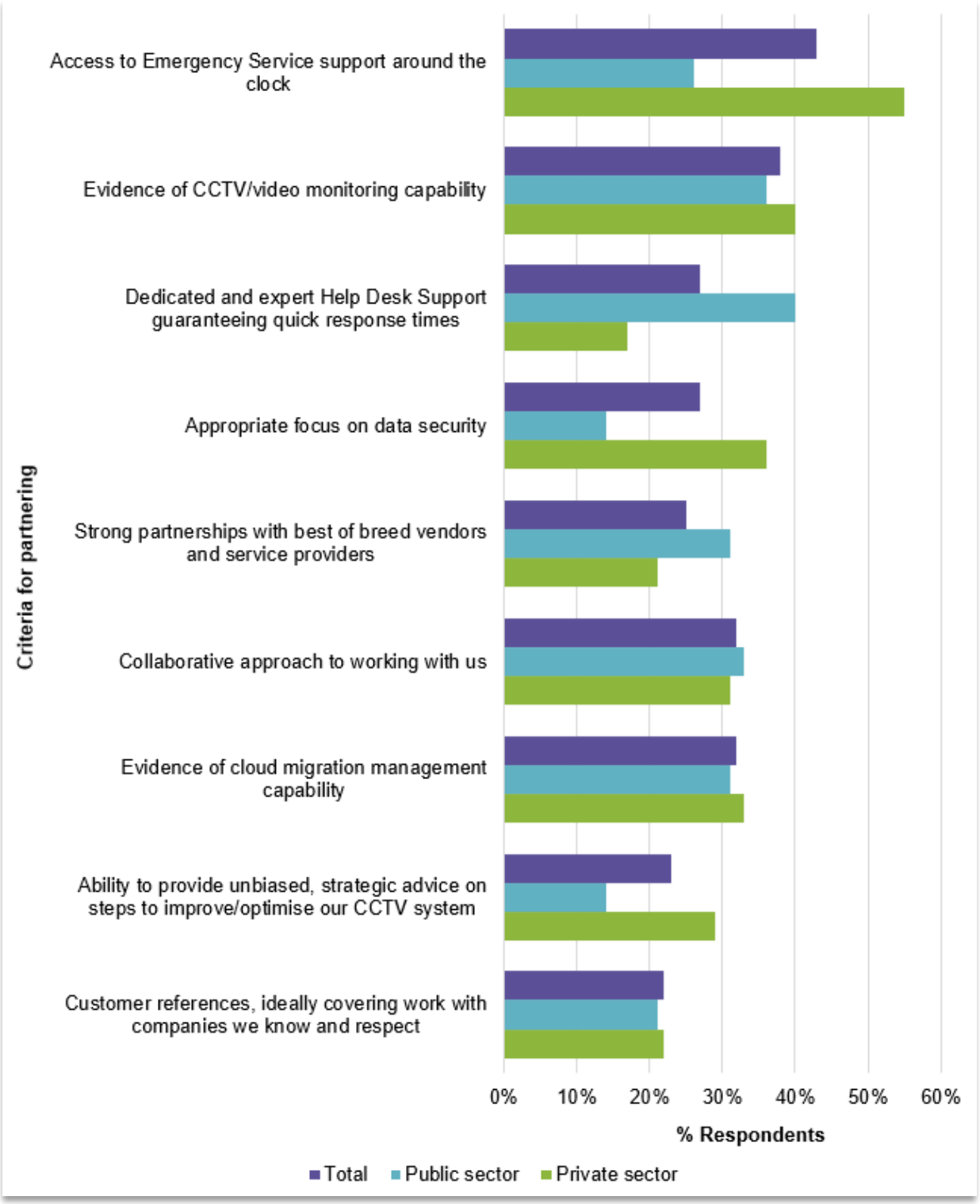


Figure 7: Provision of 'Emergency Service' support and evidence of CCTV system expertise & track record remain top 2 criteria for security installer selection. Cloud migration skills are already demanded by a third of medium and large businesses.

Ground rules for solid partnering

Very often, ICT teams will want to gain specialist outsourced support to help expand, renovate, optimise, or even migrate their CCTV system into the cloud. What then are the key criteria for selection, and how should these engagements work to best effect?

The key for NW Security, as one of those potential outsourced partners, is to be able to build a relationship in which we are treated as a genuine partner. It works least well when a 'short-termist', transactional, customer-supplier approach is taken from the start as this tends to set too rigid a tone for the agreement which tends not to work well for either party in the end.

Partnerships are built on collaboration and a strong dose of 'give and take'. So, for example, our project managers will encourage able in-house teams to manage routine, physical on-site maintenance of cameras and video management software updates. When we do need to resolve a more complex issue, we recommend being open to diagnosing and fixing it remotely wherever possible.

Remote support first

9 out of 10 support queries can be resolved through gaining remote access into your security system to perform a configuration setting check or change. Most security system problems are diagnosed quicker via remote access. We have all the IT tools we need on our helpdesk team's PCs to diagnose and fix most issues within minutes, rather than waiting potentially several hours for us to get to site.

If they are comfortable with a remote-led support service, this can save clients considerable amounts of money. It's a service approach which has gained many followers since the pandemic broke, but we've been doing it this way for years to

What to look out for in your outsourced team

Solution design capabilities

Command line configuration capability

IT networking proficiency

Cyber security skills and following best practice for hardening systems

save the customer time and money, while reducing our carbon footprint.

If, however, clients insist on untriaged physical attendance at site when there is a problem with the system - and around the clock, we need to regard this as a premium service and must charge accordingly.

Specialist versus generalist

Be cautious about reaching out to a security installer which claims to have generalist security fitting capabilities. Do they offer CCTV, fire alarms, smoke detection and suppression, intruder alarms and electronic lock fitting services? Find out which of these is their core competence by asking what they focused on at their foundation. This is, more than likely, still their core expertise today.

Credentials check

In addition, all security systems have demanded new skills as they have been networked. Have they got the IT and networking skills, the proven cyber security skills and relevant certifications; and are they partnered with the vendors that you already have in place or are planning to put in?

Look out for whether they are a Cyber Essentials Plus, SSAIB certified company and have a WCS ISO 9001 quality management certification covering key services that you are interested in using.

Summary

Optimising CCTV systems needs to start with getting the basics right and making sure you are correctly resourcing the support you have. This is always important. However, it is all the more important if you are looking to migrate from traditional CCTV infrastructure to IP video monitoring. It's also critical if you are contemplating moving your CCTV system into the cloud as, according to our research, many firms are this year.

You must think hard about the credentials and service level agreement requirements governing selection of any expert security integration and support partner. Exploring their background, credentials, certifications, and attitude to customer support is all critical if you decide to go down this route.

Optimising CCTV systems needs to start with getting the basics right and making sure you are correctly resourcing the support you have

5 – How optimised are firms' CCTV systems?

NW Security put several questions to CCTV system decision-makers to ascertain the overall optimisation levels of systems across businesses with more than 50 employees across the country.

One of the most significant findings of the NW Security CCTV management study was that 97% of medium and large-sized businesses wanted to make significant improvements to their existing CCTV systems.

Faster access to key CCTV data important for optimisation

Nearly 1 in 5 medium and large-sized firms (19%) wanted their CCTV systems to find and retrieve footage of incidents easier and quicker. This group expressed dissatisfaction that it was taking too long to find the correct video following known security incidents.

False positives down

Almost 1 in 10 firms (8%) wanted to dramatically reduce the number of false positives that their CCTV systems were flagging – admitting that checking up on false alarms was consuming too much of their time.

Frank Crouwel, Managing Director of NW Security explained:

"This is better news than it might seem. False positives used to be a massive problem in first generation video analytics software, but it should be possible now to deploy and tune next generation video analytics tools to reduce false positives dramatically."

Connected with this comment, a further 8% of firms captured by NW Security's market study wanted their CCTV systems to be upgraded to add intelligent video analytics to better support post-event decision-making.

Thanks to next generation video analytics tools, CCTV system owners are more able to drastically reduce the rate of costly false positives

Camera redeployment for COVID-19 compliance

Many firms questioned in our survey wanted their CCTV cameras to support corporate initiatives to enable a safe return of staff and visitors to their workplaces. CCTV Systems have the potential to be put to work to support key elements of COVID-safe back to the office initiatives which are being planned in earnest now.

We captured some key areas where the people in charge of CCTV systems were considering putting them to work to aid the safe return of office-based working.

User training requirement

NW Security attributes the fact that 1 in every 5 firms questioned in its study were struggling to access relevant video recordings following incidents to the need for more comprehensive user training.

NW Security highlights the importance of user training when new video management systems (VMS) are being deployed or when new staff are joining:

“VMS search capabilities are generally very good at helping the user locate relevant video sequences today. But operatives need to know how to use the on-screen tools to the fullest.

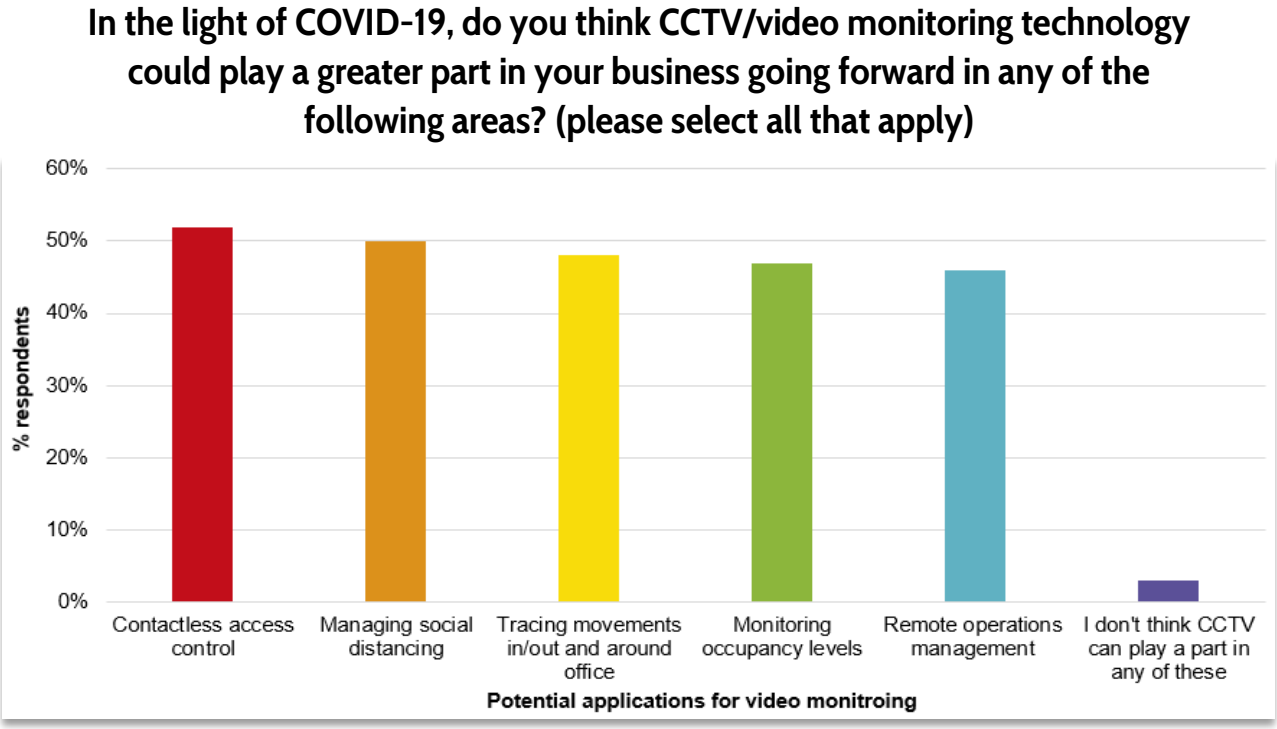
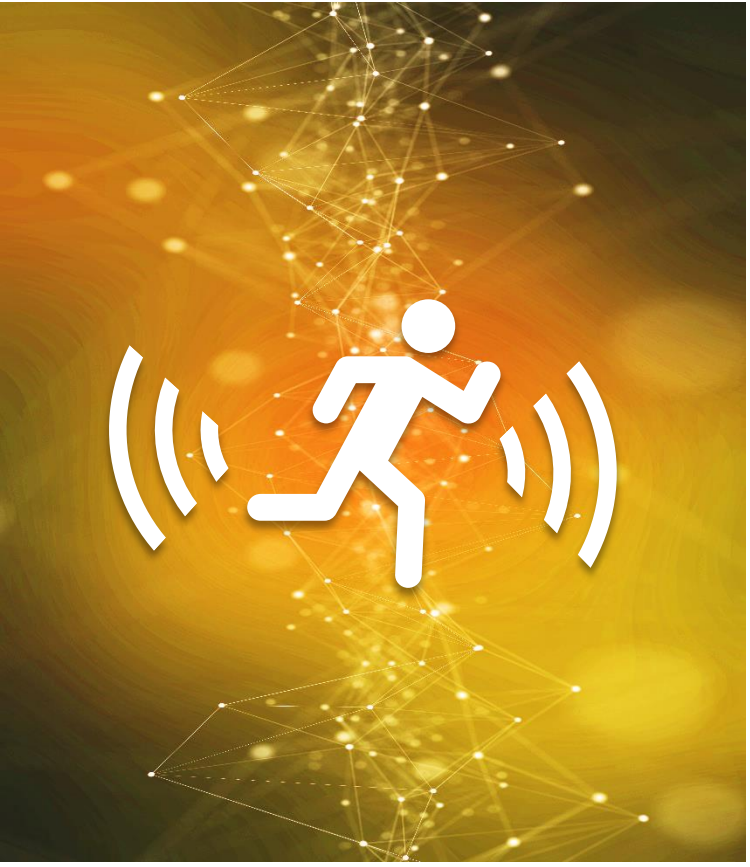


Figure 8: CCTV systems judged most useful for managing social distancing and supporting contactless access control.



Using motion detection to set up relevant event triggers can reduce the amount of data captured by over 50%

"It's also worth looking at how much 'empty data' you are collecting. It's easy enough to set up recording on relevant event triggers using motion detection for example, so that only relevant activity is collected. This configuration change often reduces the amount of data captured by over 50%," Frank Crouwel added.

GDPR compliance demand

In NW Security's study, 5% of firms were concerned that their video systems needed to have GDPR compliance baked into them to ensure compliance in the way video monitoring data is collected, stored, accessed, processed, and deleted.

Over 1 in 10 (12%) wanted to improve back-up systems around network video recordings to ensure no vital recordings were lost.

6 – Best practice tips for CCTV system optimisation

1. Integration must be driven by ORs

Over a third (36%) of firms wanted their CCTV systems to be integrated better with other security-related systems such as access control, fire and intruder alarm systems.

NW Security queried why so many firms wanted full system level integration between intruder and fire alarm systems with CCTV. It believes some of this demand tends to come without considering real relevance for individual companies' security needs.

Businesses must work out the real operational requirements (ORs) of every camera they have installed. Then they should base modifications and integrations on what is really needed in security terms.

Frank Crouwel again:

"If you're not careful, you can end up with a system which is over-specified and underperforming. It's easy to over complicate through integration. You can actually create more vulnerabilities by doing so.

"The other factor at work here is vendor hype. Marketing materials from vendors endlessly promote the twin mantras of innovation and integration. However, the reality on the ground is that getting systems to work well together is still difficult work. It can still be challenging to maintain systems over the long term due to often unsynchronised software and firmware updates."

> "Integration should be driven by a genuine Operational Requirement, not just by the desire to integrate different technologies for the sake of it."
>
> Frank Crouwel

2. Camera-level configuration critical

When planning to improve the effectiveness of existing CCTV systems, NW Security advocates a strong focus on camera-specific configuration from the start. Each camera deployed needs to be configured in line with a company's Operational Requirements (ORs).

"However, many ORs we review rarely have sufficient granularity. In other words, they don't state what each camera is supposed to be capturing precisely – what threat(s) they are deterring or preventing, or exactly what business information is required," Crouwel emphasises.

Worse, many companies (partly because of this lack of forethought and documentation) just apply a blanket set up to all cameras: applying standard frame rates and resolution across their entire CCTV estate, for example.

It may seem onerous to document why each camera you have installed is being deployed. However, it's crucial work considering that it is likely to be there collecting video recordings for over five years before it's considered for replacement or decommissioning.

It may seem onerous to document why each of your cameras is being deployed, however it is crucial work

3. ORs also vital for GDPR compliance

The Information Commissioner's Office (ICO) demands OR information anyway. Companies must justify why they need a CCTV camera in each location where one is installed, and whether any other options that were less intrusive could have been deployed.

As part of the Data Privacy Impact Assessment (DPIA), the ICO demands a document about how the CCTV will be used and how long you will keep the recordings.

You should also explain how you plan to keep the recordings secured, and the responsibilities of your staff in relation to CCTV. There are lots more requirements detailed on the ICO's website and you must register with them also.

Therefore, spending more time on more detailed planning - and documenting your OR for each camera - is a prerequisite for staying within the law and achieving good outcomes.

4. No default setups

Connected with this focus on ORs, it is important when cameras are set up originally not to deploy them on standard, default ‘out of the box’ settings.

Avoid ticking through all the standard settings to get cameras live as quickly as possible. This approach normally renders your systems un-optimised. It can also expose them to cyber security network vulnerabilities.

This lazy option frequently costs the business more money and operatives more time because, very often, those inefficiencies are not spotted for months or even years. In some cases, inefficiencies are never identified and rectified.

Make sure the camera equipment and software you have selected offers ‘Advanced Settings’ which enable the necessary granular configuration. It may cost a little more for devices and software which offer this granularity and flexibility, however in larger CCTV systems it could save thousands of pounds in the long run in terms of bandwidth usage, storage space, even RAM and CPU utilisation.

5. Review initial configurations

Review the camera and video management system configuration about a month after the initial system has gone live to make sure cameras are delivering the right video evidence, to the right quality. Often at this stage, managers running CCTV systems uncover new uses for cameras which require configuration changes.

Make sure the camera equipment and software you select offers advanced settings for granular configuration

For example, a camera deployed to monitor footfall through a covered shopping centre might find that certain cameras need to be used to provide evidence in a rising number of ‘slip and fall’ insurance claims. Because evidential requirements are more onerous in this case, the cameras covering certain areas may need to deliver higher quality video and hold it for longer.

It's also advisable to review performance of cameras installed outdoors as seasons change. So as winter approaches, cameras can be

checked for performance in lower light conditions, evening glare or during heavy rain. Is the fact that the sun is lower for longer creating a vulnerability in some areas at dusk? Video recordings must be reviewed and the cameras and cabling itself checked for evidence of water ingress or vandalism for example.

6. Camera firmware and VMS

Make sure camera firmware is kept up to date. At least once a year VMSs should also be updated to the latest version, complete with cybersecurity patches. Firmware and software updates often contain performance enhancements, so staying on top of this is critical for running an optimised system that will deliver for you.

7. IT infrastructure double check

Companies running CCTV systems must ensure underlying IT infrastructure is adequate and sufficiently specified to handle the large volumes of video any system will require. Video data is very different from other types of data flowing through a corporate network. Servers with the latest Windows operating system, storage devices and networking equipment will all need to be specified and configured correctly for optimum video data processing.

Summary

It is clear from our findings associated with optimisation of CCTV systems that expectations are rising rapidly and there have been notable successes in recent years in areas such as reducing false positives.

However, the findings also reveal a need to get back to basics - investing in tighter configuration of systems as well as more rigorous user training so that all security teams can put increasingly sophisticated VMS to work.

Configuring cameras in line with defined ORs also remains an often-neglected area for optimising CCTV systems. Setting these correctly has gained importance now that GDPR makes it a legal requirement.

The findings indicate a need to get back to basics - investing in tighter configuration and more rigorous user training

7 – Final thoughts

Perhaps one of the most significant findings of this study of medium and large businesses running CCTV systems across England, is that the CCTV to Network Video tipping point has now been breached in all sectors. Some markets like construction and retail, distribution and logistics have almost completely replaced ageing analogue-based CCTV systems.

Now that this tipping point has been reached, the way is finally clear for wider adoption of some of the latest video analytics and AI-driven functionality.

However, wider adoption of more complex technology and the availability of a growing number of VSaaS providers is creating a pressure for Facilities Management and Security teams to hand over more of the responsibility for video monitoring to IT departments.

Many IT departments of medium and large firms, up and down the country, are simultaneously going through their own quiet revolution by moving more enterprise applications and services into the cloud. Some are even ‘Cloud First’ evangelists who require incredibly compelling arguments not to move all networked systems into the cloud.

That said, we are not anticipating that wholesale movement of CCTV systems into their IaaS of choice will make sense for any but the largest and most sophisticated video monitoring system owners.

However, the speed of movement of CCTV systems into the cloud may take everyone by surprise bearing in mind that this study uncovers the fact that over 40% of all firms captured in our study said that their cloud migration plans had been accelerated as a result of the operational pressures created by COVID-19.

The way is finally clear for wider adoption of some of the latest video analytics, AI-driven functionality, and cloud CCTV technology

All this change, whatever it's speed, creates increased demand for security specialist integrators and consultants who have the right mix of physical security system configuration, network integration and now cloud migration capabilities.

While we are waiting for firms to press the button on their CCTV cloud migration projects, we can expect to remain very busy helping businesses optimise the systems they have today; re-configuring systems to underpin health and safety of workspaces in a post COVID-19 world in which we will have to remain watchful for new variants and outbreaks and mitigate against these as far as possible – ideally without sending everyone home.

Research outline

Nationally-respected market research firm, Opinium executed this survey which was completed by 101 IT decision makers of firms with more than 50 employees based in England, between 8th and 14th September 2020. Only firms with CCTV systems were invited to complete the 15-question survey.

Respondents were heavily weighted towards decision-makers in senior operations roles, as well as security and IT heads, all employed by medium (with 50-249 staff) or large-sized firms (with 250 or more staff) based in England. 29% of respondents were IT Managers, 33% IT Directors, 10% CTOs, 8% CIOs and 7% Operations Directors. The balance were Operations Managers or equivalent.

A copy of the raw data from this study can be provided by contacting Miles Clayton at Agility PR on **01992 587 439** or emailing him at **miles@agilitypr.co.uk**

About NW Security Group

NW Security Group is one of the leaders in IP video technology in the UK and it strives to remain at the forefront of technological advancement in the security market going forward. NW Security has built highly reliable and well specified services for networked and cloud-based CCTV systems, working with a range of leading vendor partners. NW Security can be reached via **www.nwsecuritygroup.com**, via email on **enquiries@nwsecuritygroup.com** or by calling **0151 633 2111**.