Cloudview®

A **Survey** on the use of **Video** in **UK Social Housing**

Intelligence Report | November 2016

2016

Contents

Executive Summary

This report, based on a comprehensive online survey of a cross-section of UK social housing providers, looks at how and why CCTV is used, the limitations of existing analogue systems, data protection loopholes and concerns and the advantages of cloud-based CCTV. Some of the key points include:

- **Use of CCTV** – Of the housing providers covered in Cloudview's survey, 97 per cent either already use some form of CCTV or are actively considering doing so.

- **Reasons for using CCTV** – Protecting their premises and buildings is seen as the most important reason for housing providers' use of CCTV, followed by monitoring access to buildings and deterring potential criminals.

- **Concerns about CCTV** – Image quality is housing providers' most pressing concern about using CCTV. Data security and compliance with the associated data protection legislation are the next most important concerns.

- **CCTV image quality** – As mentioned above, 99 per cent of housing providers rated the quality of CCTV images as being significantly important.

- **Data protection & hacking** – Almost 60 per cent of respondents are aware that their CCTV systems are vulnerable to being hacked, although many don't know how to make their system more secure. 15 per cent of CCTV users are completely unaware of their vulnerabilities.

- **Cloud-based CCTV** – More than half of the respondents would consider using the cloud if it made their CCTV system safer, more reliable and easier to use.

- **Internet of Things** – Despite surveillance cameras being the second most internet connected device, all of the top eleven concerns about using CCTV could be solved by adopting an IoT solution.
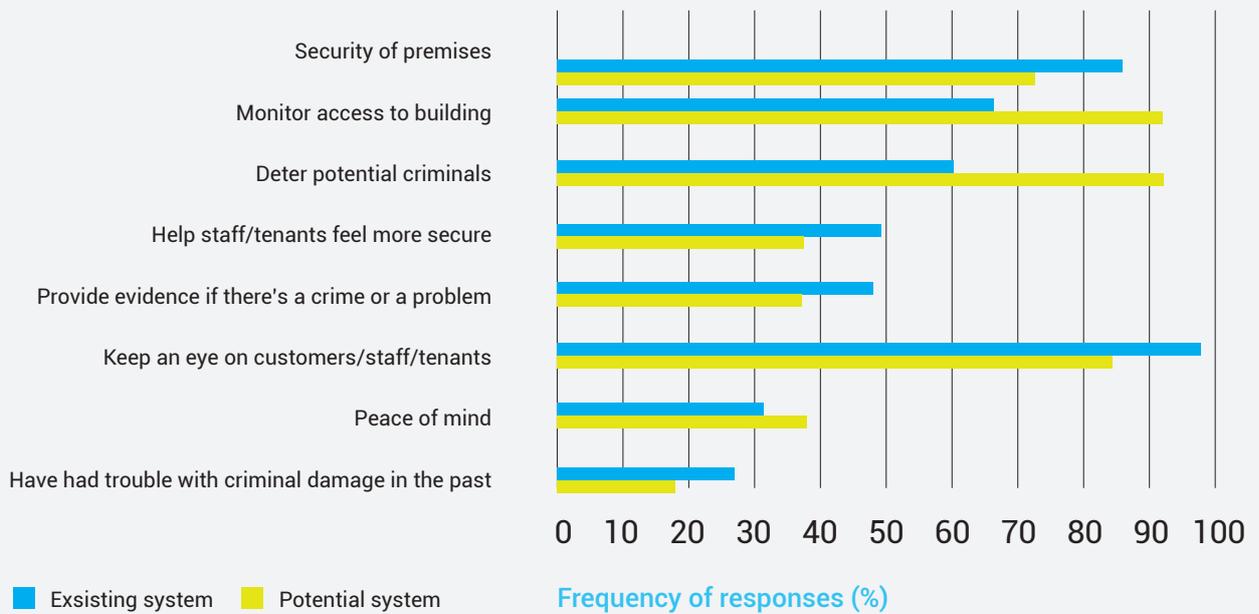
Further information about Cloudview's cloud-based video surveillance system can be found at: www.howtocloudview.co

Does your organisation use CCTV?

3%

11%

86%

- Yes
- Not at the moment, but it's being considered
- No, and it's not being considered
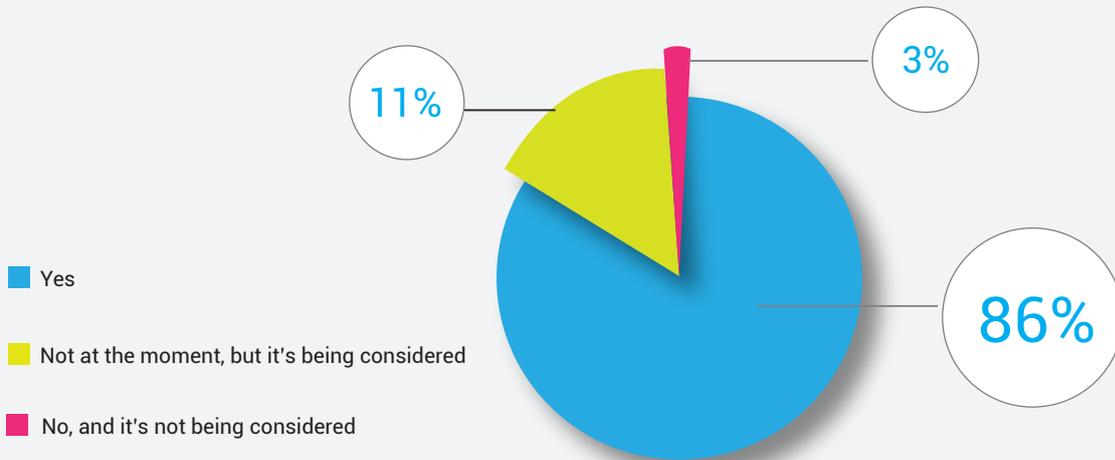
Of the housing providers covered in Cloudview's online survey, 97 per cent either already use some form of CCTV or are actively considering doing so. Only three per cent have no plans to install CCTV, most likely due to the specific nature of their housing stock.

Why does your organisation use CCTV?

Security of premises

Monitor access to building

Deter potential criminals

Help staff/tenants feel more secure

Provide evidence if there's a crime or a problem

Keep an eye on customers/staff/tenants

Peace of mind

Have had trouble with criminal damage in the past

0 10 20 30 40 50 60 70 80 90 100

- Exsisting system   Potential system   **Frequency of responses (%)**

For housing providers already using CCTV, protecting their premises and buildings is seen as the most important reason for its use, followed by monitoring access to buildings and deterring

potential criminals. This contrasts with the views of housing providers that have yet to install CCTV, who place greater importance on monitoring building access and on CCTV's value as a deterrent to potential criminals.

The second tier of reasons for using CCTV are typically to help tenants and staff feel more secure, and to provide criminal evidence. In each case, existing CCTV users rated these factors more highly than organisations only considering the use of CCTV.

The least important reasons for using CCTV were peace of mind, keeping an eye on customers, staff or tenants and previous criminal damage.

What are your biggest concerns with your CCTV system?
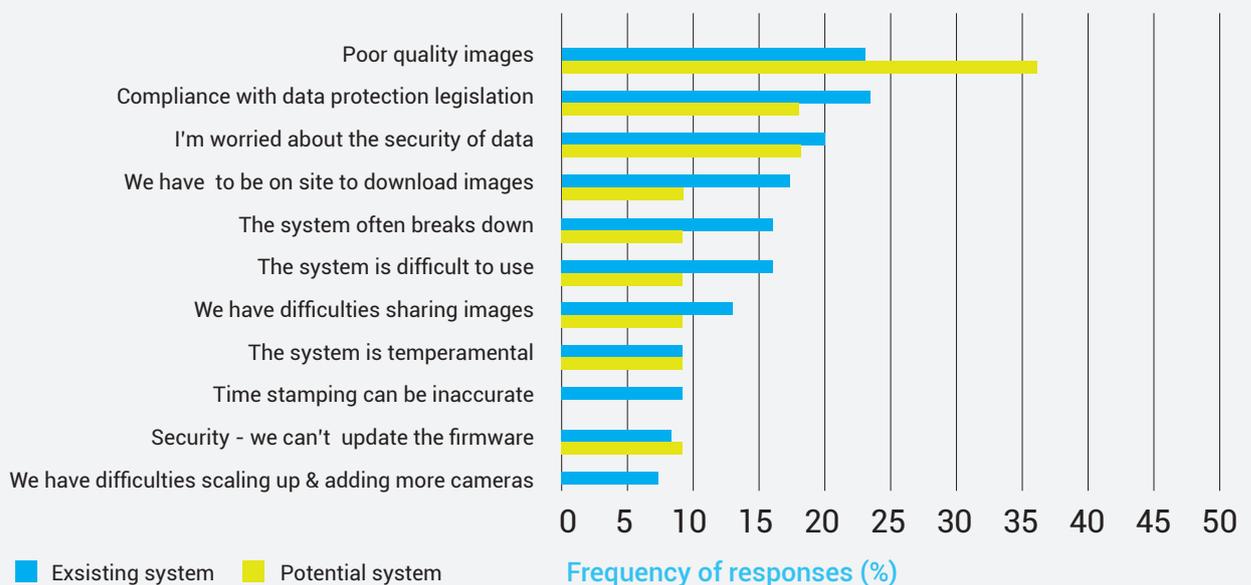
The quality of images stands out as housing providers' biggest concern about using CCTV, and is an even stronger concern among those still considering whether to install CCTV. Data security and compliance, with the associated data protection legislation, are the next most pressing concerns, particularly among experienced CCTV users.

These three factors are closely connected. To ensure compliance with the DPA, data recorded with the purpose of identifying individuals performing criminal activities must be of sufficient quality to do so, which means that if the image quality is poor, an organisation risks breaching the legislation. The CCTV data must also be stored securely to prevent unauthorised access and hacking, something which is a concern for both existing and potential CCTV users.

It is interesting to note that the actual practicalities of using CCTV, such as needing to go on site to download images, ease of use, reliability and the sharing of images, are all rated as much greater concerns by housing providers already using CCTV, whereas potential CCTV users are less aware of, and have yet to find out, these difficulties. Ironically, in order to make the system and data secure, accessibility is sacrificed, making the job of the user even more difficult.

Issues	IoT solution
Poor quality of images	✔
Compliance with data protection legislation	✔
I'm worried about the security of the data	✔
We have to be on site to download images	✔
The systems often breaks down	✔
The system is difficult to use	✔
We have difficulties in sharing the images	✔
The system is temperamental	✔
Time stamping can be inaccurate	✔
We can't update firmware against cyber-attacks	✔
We have difficulties scaling up and adding more cameras	✔

Accessibility and sharing of images are issues that could be addressed by connecting CCTV cameras to the IoT. According to Gartner*, we should expect 6.4 billion devices to be connected before the end of this year, while it estimates it will reach 20.8 billion by 2020. Surveillance cameras are already the second most prevalent internet connected devices, yet this appears not to be the case with those used in the housing sector. Using the IoT would address all of the 11 issues highlighted in this survey, from access to accurate time stamping.
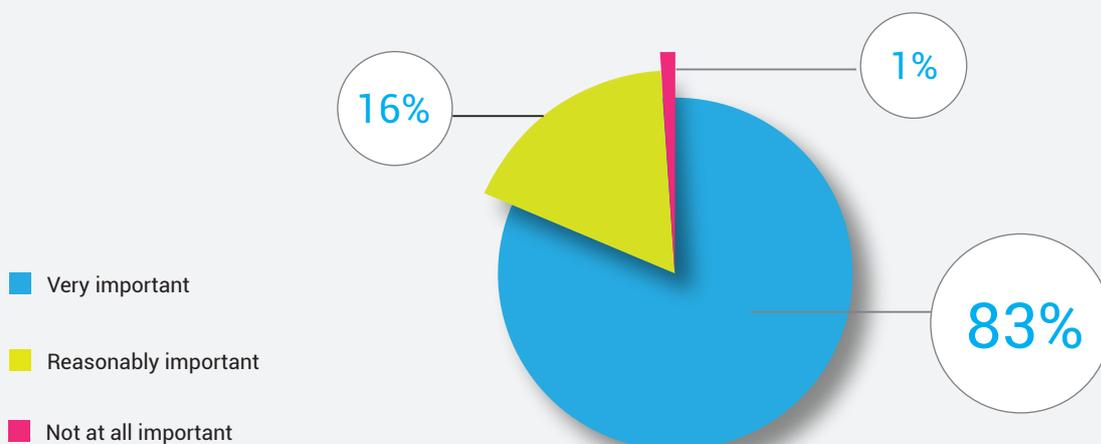
The expressed concern about the sharing of images is another issue that affects data protection and compliance. Individuals have a right to request a copy of CCTV footage where they are the focus, and/or are clearly identifiable; if their request is valid, the data must be supplied within 40 days. If the recordings are aimed at preventing criminal activities, then they should also be easily accessible by the police. The footage also needs the correct time stamps and qualification against tampering. Organisations who find it difficult to share images securely are therefore at risk of breaching data protection legislation. Here, too, the IoT would solve the problem.

The areas of least concern include the time stamping of images, firmware updates and adding additional CCTV cameras. There is no point in having a high-quality image if the time it was recorded is inaccurate; it is both unusable for many purposes, and is another potential breach of the Data Protection Act. The Information Commissioner's Office points out that if data is to be recorded, it must be done accurately as well as securely in order to be used properly, otherwise its capture is unjustified. With regards to firmware, there seems to be a lack of understanding of the security risks of not implementing updates and patches. Out-of-date firmware can leave systems open to hacking, as new security threats are being developed all the time.

These are all issues that Cloudview's IoT system addresses. As well as providing high-quality images, all data is fully encrypted and time stamped, then securely stored in a cloud-based, protected environment for access by authorised personnel via any web-enabled device. It can also handle large volumes of data, is highly scalable to accommodate future growth, reliable and robust, and makes the sharing of images very easy, all within a highly-secure, proven technology platform.

*http://www.gartner.com/newsroom/id/3165317

How important do you think the quality of CCTV images are?

16%

1%

83%

- ■ Very important
- ■ Reasonably important
- ■ Not at all important

Echoing users' concerns about image quality in the previous section, 99 per cent of respondents rated the quality of CCTV images as either very important or reasonably important.
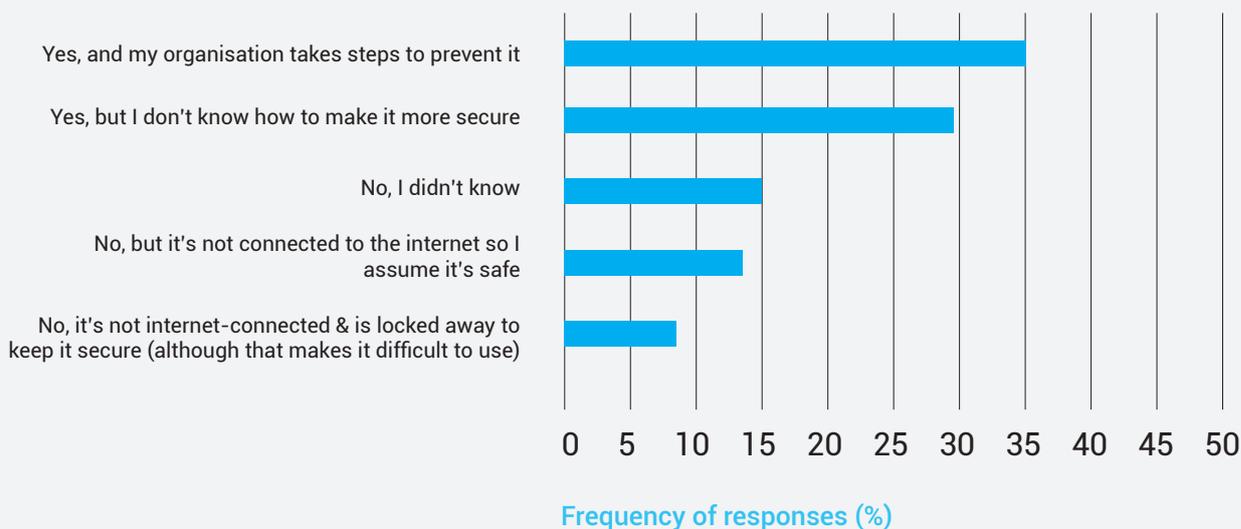
This is because of (or in spite of, depending on your perspective) the low quality and unreliability of the images from most housing providers' CCTV systems. Users remain firmly attached to analogue technology; only around one fifth of new CCTV installations are digital, and the installed base is highly reluctant to change.

Users typically give two main reasons for this: one, it would require an expensive 'rip and replace' of their existing infrastructure, which is simple to install and works well; and two, they believe that digital CCTV is more complicated, insecure and expensive to install.

Again, it is important to point out that data recorded with the purpose of identifying individuals must be of sufficient quality to do so – which means that if the image quality is poor, an organisation risks breaching data protection legislation.

In contrast with most housing providers' existing and often out-dated CCTV systems, Cloudview's system will work with both old analogue CCTV cameras and newer 1080p IP cameras, enabling housing providers to 'federate' their old, and additional new, camera feeds into a single account. There is no need to rip and replace cameras, or cabling, as the Cloudview adapters can simply be added to existing cameras. Cloudview also provides evidence-quality snapshots and high-definition video.

Did you know that traditional CCTV systems can be hacked into and used to steal valuable corporate data, which would mean that your organisation contravened its responsibilities under the Data Protection Act to protect the data from unauthorised access?

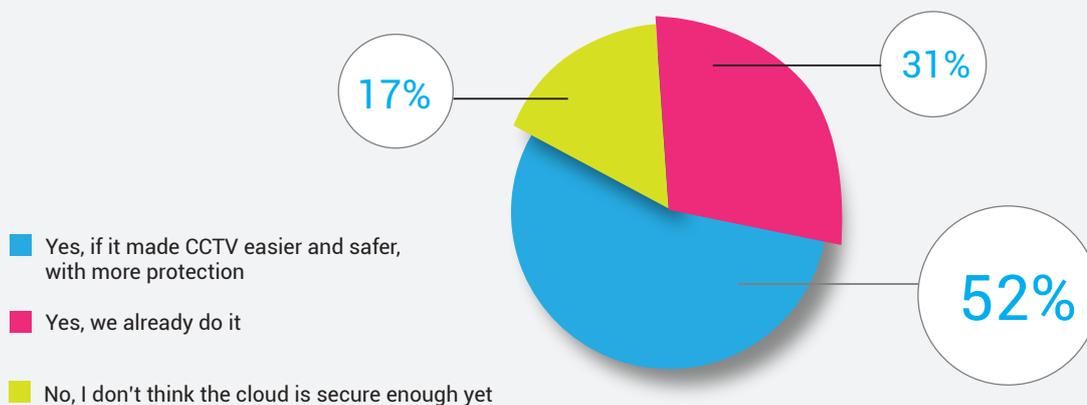|	Frequency of responses (%)
Yes, and my organisation takes steps to prevent it	~35
Yes, but I don't know how to make it more secure	~30
No, I didn't know	~15
No, but it's not connected to the internet so I assume it's safe	~14
No, it's not internet-connected & is locked away to keep it secure (although that makes it difficult to use)	~9

Frequency of responses (%)

Almost 60 per cent of respondents are aware that their CCTV systems are vulnerable to being hacked, although around 25 per cent don't know how to make their system more secure.

15 per cent of CCTV users are completely unaware of their vulnerabilities and almost the same number mistakenly assume that their system is safe simply because it's not connected to the internet. However, systems are equally insecure if they are connected in some way to a corporate network (such as via a DVR). The solution is to combine the IoT with cloud technology, and to have the necessary security safeguards built in.

Around eight per cent of respondents have internet-free systems that are locked away, despite such measures making the system much more difficult to use effectively, with data retrieval more time-consuming. This can also make it difficult for organisations to know whether their CCTV system is actually even working. In addition, if CCTV systems are not connected to the internet, it is difficult to take advantage of any new firmware revisions that may deliver enhanced security, new features and other additional benefits.

Because the DVRs storing data in traditional CCTV systems can be vandalised and stolen, would you consider using the cloud to record, store and access CCTV images?

17%

31%

52%

- Yes, if it made CCTV easier and safer, with more protection
- Yes, we already do it
- No, I don't think the cloud is secure enough yet

Just under a third of respondents say that they are already using cloud-based technologies to record, store and access CCTV images. However, Cloudview's experience suggests that this may be an unintended exaggeration because cloud is still very cutting edge in the CCTV market. It is more likely that they are using remote access to view live feeds and occasionally download, or back up, data (with all its difficulties and security failings).

More than half of the others would consider using the cloud if it made their CCTV system safer, more reliable and easier to use. Almost a fifth of respondents think that the cloud is not yet sufficiently secure, despite most existing remote access services being fraught with security issues and demanding considerable technical expertise to tie down properly.

Their concerns have some foundation; while the cloud, in theory, offers greater security, it is important to understand that not all cloud-based video solutions are secure. Many use the same IP connection and 'port forwarding' techniques as old-fashioned DVRs, leaving CCTV data equally insecure.

However, these concerns can be addressed by the latest generation of cloud-based IoT solutions, which also enable analogue cameras to be connected to the cloud. Cloudview's IoT solution only allows outbound connections. And because the Cloudview adapter only has to perform a fraction of the functionality of a full DVR, it is much less powerful and hence much less attractive to a potential attacker.

Conclusion from Cloudview

In Cloudview's experience, 'native'/legacy CCTV systems give limited service as a deterrent, and as a source of evidential information. This is because perpetrators often simply assume that CCTV is unattended or broken and after a while ignore it completely. Using either remote access, which introduces an additional risk of hacking, or direct access to obtain evidential footage is time consuming and expensive and therefore is often avoided except in extreme circumstances. In many cases, external contractors are needed to obtain CCTV footage for housing providers because natural staff attrition means that technical knowledge is lacking.

Responsibility for CCTV can also be passed around different departments, meaning that important functions such as equipment maintenance (maintaining correct system times, etc.) and cyber security are overlooked.

CCTV equipment can very often be non-functional, and this isn't discovered until it is urgently needed. The next-generation Cloudview system resolves this through continual online diagnostics, with immediate alerts of any problems.

Given the choice, the housing providers encountered by Cloudview said that they would like to have access to visual data more readily in order to resolve not only big criminal-type problems, but also small day-to-day problems, such as checking on the attendance of contractors, the cleaning of communal areas, health and safety practices being observed, and that vulnerable residents are being protected from daily risks. This is simply not practical with regular CCTV but can be enabled with IoT-based cloud services such as Cloudview.

There is a trend towards consolidation in the housing sector, and this in turn means that housing providers are now paying more attention to the use and security of their data (including CCTV). This focus on data security strongly favours cloud systems which resolves many of the security and administrative problems caused by disparate, old-fashioned CCTV systems.

The ongoing cost of CCTV, and achieving value for money, is a big concern for all housing providers who want to reduce their operational costs and find ways for their staff to work more efficiently and without unnecessary risks. In this area, Cloudview estimates that the cost of running its cloud-based video surveillance system is less than half the cost of regular CCTV systems.

About Cloudview

Cloudview provides the world's first corporate-grade, secure, cloud-based video system. It uses the Internet of Things (IoT) to connect CCTV cameras across multiple locations, encrypting and storing footage securely in the cloud from where it can be viewed, managed and shared by authorised users on any smartphone, tablet or PC. Cloudview adapters can also be integrated with other IoT devices to add visual data to their capabilities.

Cloudview works with a number of housing associations in the UK, providing secure and cost-efficient video surveillance and is the only CCTV product to have been awarded 'Police Preferred Specification' status.

Cloudview was highly commended in the 'Internet of Things Solution' category for the Computing Vendor Excellence Awards 2016 and has been shortlisted for the 'IoT Security and Data Encryption' categories in the upcoming Computing Security Excellence Awards.

The firm was founded in 2012 and is headquartered in Hampshire, with development teams in Amman, Jordan and Northampton, England.