The need for organizations to store more data for increasing lengths of time is symptomatic of our litigious society where closed circuit television (CCTV) is being used as a method of maintaining records for legal, insurance, financial or health and safety purposes. This white paper discusses the storage needs of CCTV security video, which are affected by a wide range of factors—ranging from political and societal to technical and economic. Faced with multiple influences and options, organizations must have an appropriate strategy and the proper technology in place to address their specific needs. Fortunately, new developments in storage technology make it possible for organizations to simultaneously establish practical and highly effective backup and archival practices.

Fiction Becomes Reality

George Orwell was right—and wrong. In his career-defining work, Nineteen Eighty-Four (1984), he portrayed a totalitarian future society where everyone is under constant surveillance and the ruling elite wield total power over the inhabitants for their own sake.

However, while society today—25 years after the date in Orwell’s novel—is filled with vast numbers of closed circuit television (CCTV) cameras, the widespread use of security video has not resulted in totalitarian states where “Big Brother is watching” and personal freedom is limited.

On the contrary, CCTV and security video are now being used in a widespread number of positive ways that have made society safer and more secure. Most notably, CCTV has been an effective tool in crime fighting, particularly as an aide to detection when used as part of a wider strategy. Whether operated by the police, local authorities or private business owners, CCTV has been instrumental in identifying and bringing to justice all types of criminals—from those who commit serious, high-profile crimes like terrorist incidents to those who commit a host of lesser, more “ordinary” crimes, such as vandalism, illegal trespass and robberies.
In fact, it has now become a common practice for security video footage of a crime to be released to the public as an aide in identifying and ultimately capturing a suspect. At the same time, working behind the scenes, if the police receive a report of a suspect fleeing a crime scene in a blue car, for example, security video can be used to automatically search analytic data based on the color of the car in virtually any part of a city and within any timeframe.

Moving Beyond Police Work

In addition to these more visible uses, CCTV has expanded from police applications into all kinds of security applications across a wide range of industries, such as transportation, energy, food and beverage, as well as education.

Increased efforts to protect critical airport infrastructure following the 9/11 terrorist attacks, for example, have led to increased budget allocations for CCTV surveillance systems to combat security threats and protect airport perimeters. The United States, Western Europe and Asia Pacific nations as well as certain countries in South America have all installed strong, proactive security solutions to protect both travelers and airport personnel. In addition, railroads have installed CCTV systems that offer improved safety, such as for the detection of platform crowding, dangerous behavior and trespassing on tracks, as well as for terrorism and emergency prevention and detection, including the detection of luggage left unattended on platforms.

At the same time, the oil and gas industry has responded to both the threat of terrorist attacks on chemical plants and oil refineries as well as the growing concern and awareness of general security and processing safety issues. These same concerns extend to the food and beverage industries as well. Restaurants and food establishments have embraced CCTV both for health and safety reasons as well as for anti-theft and security reasons. CCTV monitoring now includes kitchen food preparation to avoid embarrassing “there’s a fly in my soup” scenarios, to ensure that financial transactions at the counter are rung up and processed properly and that parking lots are safe and secure.

In addition, an increasing number of schools, colleges and universities are now using CCTV to help monitor and discourage student misbehavior, such as truancy, smoking and substance abuse. At the same time, CCTV is being used to proactively prevent incidents and improve responses to incidents that affect the personal security of staff, pupils and visitors. Schools face a variety of risks from potential intruders who may threaten students and staff to vandals and arsonists intent on damaging school property. For schools, the outcomes can be particularly disastrous, not only because of the costs involved, but also more significantly in terms of the lost educational opportunities for students. A generation ago, there might have been an occasional theft or fight at school, but the greater incidence of bullying today, with increasing levels of violence, has meant that safety and security have emerged as one of the foremost concerns for everyone involved in the education field.

Security Video Is Going Tapeless

According to Surveillance-source.com, many CCTV applications are now moving away from traditional videotape-based systems and are increasingly embracing tapeless digital CCTV surveillance systems that digitally record information. This move eliminates the costs and headaches traditionally associated with videotapes, while ensuring higher-resolution digital image quality. Tapeless recording also eliminates tape shuttling to provide instant, on-demand access to critical recordings to find images or events by time, date or camera number through the use of on-screen menus and simple keystrokes.
Guide to Video Security Storage

With all of this increased use of CCTV and security video comes the challenge of how to properly store and archive the mountains of digital data that are now being captured—particularly when this data needs to be accessible to the proper authorities when needed, while still ensuring that individual privacy rights are protected. At the same time, the amount of data that needs to be stored is subject to compression ratios, image size and images stored per second. In fact, there is a drive to increase the number of images stored per second, from six images per second to 25 images per second in some installations. This is particularly urgent in homeland security and law enforcement applications where security video is required for evidential purposes.

Retention Rationale

According to an article in Hi-Tech Security Solutions, the amount of time that security video data needs to be retained can be an important factor in many issues. This data needs to be preserved for a range of purposes, from the primary reason it was created (such as monitoring a food processing line) as well as for a reasonable amount of time to recover any evidence of any other important activity that it might document (such as a contaminant entering the food processing line). Also, this data may need to be reviewed for any historical, research or other long-term information of value it may contain, such as for improving supply chain management or manufacturing processes.

According to the National CCTV Strategy report from the Home Office in the U.K., it has long been accepted that CCTV recordings should routinely be kept between 28 and 31 days before being recorded over. This time period allows the police the opportunity to recover CCTV evidence and respond to lines of enquiry that may not have been known at the time an incident was reported. This schedule also helped in the videotape recycling process by ensuring that the tape would not be used day in and day out.

With the introduction of digital CCTV systems, some system owners have moved away from the 28 and 31 days figure to periods as short as 14 days. However, this has resulted in significant resource implications for the police, which must collect the digital CCTV before the footage is overwritten. This becomes even more important in terrorist investigations, where extended periods of between 14 and 31 days are often required.

With that in mind, the police have therefore reiterated their need for 31 days of storage in the digital CCTV era, with the requirement that the recording quality should not be reduced or compromised, which could result in the recordings not meeting the “fit for purpose” criterion. On some occasions, such as cold cases and trials undergoing appeals, CCTV material has to be archived for a number of years.

On some occasions, such as cold cases and trials undergoing appeals, CCTV material has to be archived for a number of years.

— Hi-Tech Security Solutions
Guide to Video Security Storage

Too Much Data, So Little Room …

The volume of storage required on this scale understandably brings with it many problems. The use of this data for investigation, retrieval of evidence, auditing and analysis is all based on an expectation that data would be accessible. Video is storage-intensive and requires both infrastructure and management. However, for many users—from law enforcement to small business owners—the cost of a data storage system itself and managing it, rather than retention needs, will determine the time that security video information will be retained.

Security Video Retention Times

What then becomes a suitable timeframe for retaining security video? The answer will vary from industry to industry and from operation to operation. Surprisingly, sometimes there are both minimum and maximum retention duration time requirements for this material. According to Hi-Tech Security Solutions, there a number of factors that will influence how long material needs to be retained:

- National legislation. Some countries have a clearer position established through legislation protecting privacy and what are seen as reasonable periods to retain data.
- Industry legislation. The retail industry, for example, can be subject to lawsuits over issues relating to slipping on floors or faulty merchandise, and laws may allow extended time of a few months for customers to initiate a case.
- The duration it may take for somebody to respond or for something to be noticed. In some cases, a transgression or imbalance may take days to notice and for its cause to be investigated. One example is a system installed to prevent fraud at an ATM, where images may need to be retained for several weeks because a suspicious transaction may not be discovered until the victim gets a bank statement.
- Auditing and review arrangements. Some organizations routinely audit or review video footage for quality purposes.
- Time cycles or production cycles that may require that a specific time period has lapsed before something emerges as an issue. If, for instance, something is detected near the end of the month, and there is concern that it may also have occurred the previous month, then more than 30 days worth of video will need to be retained in order to detect, identify and extract the necessary information from the system before the next monthly cycle starts overwriting the information. In the same way, investigating patterns of unusual behavior or events may often require a more extensive investigation that goes back weeks or even months.
- The process or procedure for retrieving information may require confirmation and/or engagement with parties before release. Where release of data may infringe on people’s rights, obtaining clearance to release the data may take some time.

In summary, organizations need to ensure that they know what CCTV security video is important to keep, why that information is being retained or deleted and why the retention duration is important. Where there is suspicious activity or criminal action, companies should be able to find their stored and archived data easily for follow-up purposes or during investigations.

The Right Size Equipment

But having the right policy in place also means having the “right size” equipment in place. Therefore, the need to carefully plan and resource future archiving capability is crucial to the continuing and rapidly increasing volume of CCTV data. This includes a complete end-to-end process—“cradle to grave” or “camera to archive”—that considers the whole lifecycle of CCTV security video. For example, it may be important to consider how the CCTV would be used, how long it would be retrieved
Guide to Video Security Storage

and played back, how easy would it be to be played back in court and, finally, how it would be archived to enable it to be played back in 10 years or more time.

Due to the wide variety of data storage products and formats available today, businesses face a challenging purchasing decision. It is important to remember that the amount of data needed to be stored varies significantly based on the industry and the regulations required in that industry. However, this is a much more useful metric in defining the size of a business with regard to data storage requirements than the number of employees or sales revenue.

Because capacity demand increases are similar across businesses in the same industry regardless of size, it is equally important to determine how businesses administer their data storage. However, what is different is the means of dealing with meeting these capacity demands. Fortune 500 companies behave differently than small business owners; they have different priorities and different needs, but they may still be subject to the same retention timetable requirements.

A Classic Example

The new Shard Building in London is a classic example of how CCTV is being used in new and innovative ways as well as the how one company is dealing with the storage requirements of security video. The 87-floor building, currently under construction for completion in 2012, is set to become London's tallest landmark. The construction company, Mace Construction, is using high-density image per second CCTV to record deliveries, track site progress and contractor activity to more than a dozen CCTV stations that generate more than 4.8 terabytes (TB) of data per month. All this data is backed up on Tandberg Data LTO-4 cartridges and secured offsite in a disaster recovery center for seven years.

Customers who require reliable and clear CCTV footage are looking for high capacity, encrypted technology to secure their assets. With Tandberg Data’s LTO hardware and media, they are receiving this at a low cost per Gigabyte (GB)—only $0.06 per GB as compared to $0.42 per GB for disk—and one LTO-5 tape cartridge can hold a staggering 1.5TB of uncompressed data. By realizing how much CCTV data is being stored and for how long, this can amount to significant savings. Prior to the advent of LTO, users simply had to add more hard disks to extend the recording duration. Now they have a cost-effective, securely encrypted solution that also provides an IT industry standard 30-year archival life.

In addition, Tandberg Data also offers the Endurance monitoring system, which archives CCTV recordings from analog or IP cameras onto tape. Through this system, recordings are initially stored on disk for a 30-day access period and then automatically moved off onto a tape library, the Tandberg Data StorageLibrary T40+, which uses LTO-4 or LTO-5 tape. The strength of this archiving system is that the Tandberg Data T40+ can hold up to 453TB of data without requiring any human intervention. Data can then be archived on- or offsite, and it can be easily accessed and located within minutes because of barcode indexing.

The Endurance system has been installed at some extremely high-security applications within both the public and private sectors, with one client alone rolling out to 150 locations.
Guide to Video Security Storage

The Future

Looking ahead, the use of CCTV promises to become more widespread as a way of maintaining records for legal, insurance, financial and health and safety purposes. With that, more and more security video will be generated, and this data will need to be stored for increasing lengths of time.

As a leading global supplier of data protection solutions, Tandberg Data recognizes that users of CCTV surveillance systems need a storage solution that is ideally suited to their unique needs and characteristics. With a perspective gained from more than 30 years in the storage business, Tandberg Data has taken a leadership role to help companies meet the challenges of today and tomorrow.

Tandberg Data products are supported by all major operating systems and software applications to successfully integrate and operate in heterogeneous storage environments. All solutions are designed to meet the growing storage requirements of organizations of all sizes with scalability, reliability and backward compatibility features that ensure cost effective operation and long-term investment protection.