
com sur™
the missing piece of CCTV
THE FOOTAGE WHISPERER
"SEE WHAT THE CAMERA SAW"
GET THE BOOK
100+ TOPICS - AIRPORTS TO ZOOS
GAUTAM D. GORADIA

UTILITY VALUE OF COM-SUR™ FOR IT (INFORMATION TECHNOLOGY) COMPANIES

WELCOME

AUDIT HOURS OF FOOTAGE IN MINUTES FIND OUT HOW COM-SUR, THE BEST 'MOUSETRAP' WILL HELP

"Seeing is believing - See what the camera saw"

CCTV surveillance is commonly used in IT (Information Technology) companies world over, but footage is often only reviewed reactively. Our company realized this problem early-on and has developed the world's only CCTV video footage auditing software that encourages daily auditing (hours in minutes) of CCTV footage, filling the gap for a complete "workflow". The software works with existing cameras and VMS, regardless of type/brand, and provides a standardized approach for intelligent incident reporting. Our software also offers exceptional investigative capabilities.

'COM-SUR' – THE WORLD'S ONLY CCTV VIDEO FOOTAGE AUDITING, SMART BACKUP, AND STANDARDIZED INTELLIGENT INCIDENT REPORTING SOFTWARE – THE MISSING PIECE OF CCTV

COM-SUR is the world's only CCTV video footage auditing, smart backup, and standardized intelligent incident reporting software that serves as a complete workflow and force multiplier. It helps audit 24 hours of footage in minutes, reduces data size, creates standardized intelligent reports, and delivers business intelligence. COM-SUR helps unlock hidden information in CCTV footage and enables people to gain actionable intelligence, improve homeland security, prevent crime and losses, identify and mitigate threats and hazards, and improve operational efficiency. It empowers people to gain new jobs as CCTV video footage auditors and start new businesses of auditing video footage. Like MS Office, COM-SUR is an enabler that makes it easy to work with CCTV cameras in a standardized way, leading to better decision-making. It also offers exceptional investigative capabilities.

HOW COM-SUR SMARTLY REDUCES 'VIDEO' STORAGE SIZE

COM-SUR employs an innovative approach to smartly reduce the amount of video to be

audited and consequently the storage size of videos. Regardless of the video's frame rate, COM-SUR captures a single screenshot of the consolidated 'moment' of 'that' one second, when the I, P, and B frames come together. This method significantly reduces data size without sacrificing vital information. It goes without saying that when multiple cameras are displayed in a grid view, say 4x4, the storage size is further reduced since all the cameras are captured as a single image. Since no suggestion is being made to replace the actual video with screenshots, COM-SUR acts as a wonderful supportive technology both to audit (review) just 86400 frames representing 24 hours and reducing the data size at the same time.

CHALLENGES FACED BY IT COMPANIES

1. Unauthorized access:

The risk of unauthorized individuals gaining physical access to sensitive areas or equipment, such as server rooms or data centers, can lead to data breaches or disruptions to IT services.

2. Theft and vandalism:

IT companies have valuable equipment, such as servers, networking devices, and computers, which can be targets for theft or vandalism. Stolen equipment can lead to data breaches and financial losses. Perpetrators often conduct pre-operational surveillance of the target area, making it important to detect suspicious activity during this phase to prevent an incident.

3. Data breaches:

Protecting sensitive customer data and proprietary information is a significant challenge for IT companies. Breaches can occur through physical means, such as unauthorized access to servers or storage devices, resulting in the loss or theft of sensitive data.

4. Intellectual property theft:

IT companies often develop and possess valuable intellectual property, including software code, algorithms, and trade secrets. Protecting this intellectual property from theft or unauthorized access is essential to maintain a competitive advantage.

5. Disruption of IT infrastructure:

IT companies rely on their infrastructure to deliver services to clients. Physical security threats, such as power outages, natural disasters, or intentional damage to infrastructure, can disrupt operations and lead to downtime.

6. Employee safety:

Ensuring the safety of employees is crucial. IT companies may face risks related to workplace violence, harassment, or occupational hazards associated with the use of specialized equipment.

7. Compliance issues:

IT companies must comply with various regulations and standards, such as data protection laws and industry-specific requirements. Meeting these compliance obligations requires implementing appropriate physical security measures to safeguard data and systems.

8. Insider threats:

IT companies have to deal with insider threats from disgruntled employees or even unwitting staff who fail to follow proper security and safety measures.

9. Humongous growth of surveillance video:

The exponential growth of surveillance cameras has resulted in an unprecedented surge in surveillance video. Effectively managing this data has become a daunting challenge due to the massive storage capacity required, especially considering the prolonged retention periods necessary for security, incident investigation, or legal purposes.
Furthermore, the prevalence of high-resolution video with increasing megapixels compounds the storage demands, making efficient data management an urgent priority for organizations grappling with the immense volume of surveillance footage.

COVID-19 PANDEMIC

The pandemic impacted IT companies worldwide, both in a positive as well as negative way. On one hand, the pandemic accelerated the adoption of technology by businesses and individuals, leading to an increased demand for IT services and products, which led to a surge in revenue for many IT companies. On the other hand, the pandemic disrupted global supply chains and caused economic uncertainty, leading to a slowdown in IT spending by some businesses and governments. This affected the revenue and growth of some IT companies, especially those focused on hardware and traditional IT services. Guidelines were issued to prevent the spread of COVID-19, but outbreaks still occurred.

USE OF VIDEO SURVEILLANCE AT IT COMPANIES

Most IT companies have video surveillance covering the following areas:

- Entry and exit points
- Server rooms and other critical areas
- Areas housing workstations
- Corridors
- Lobby and lift areas
- Canteens/kitchen facilities
- Staff recreational facilities
- Perimeter of the building
- Parking areas

Further, the concerned stakeholders at IT companies generally need to review and analyse recorded CCTV video footage from time to time for investigating incidents and/or accidents, and other issues in order to corroborate evidence as well as assisting Police/other Law Enforcement Agencies.

LIVE MONITORING – CHALLENGES

Several IT companies have a dedicated control room with operators, set up for live monitoring of CCTV cameras. However, live monitoring comes with its own set of challenges of video blindness, poor attention span, boredom, operator bias, false alerts, and so on.

Moreover, these cameras continuously capture and record humungous amounts of video data. It therefore becomes a daunting task for the operators to review and analyse this data whenever the need arises. Thus, it may be noted that benefits from video surveillance systems can accrue only when they are used optimally, suggestions for which are enumerated further on, in this document.

COMPLIANCE - GENERAL

Conformity or compliance in any organization means adherence to laws and/or rules and regulations, various standards, as well as data storage and security requirements as laid down by government bodies, governing bodies of the respective industry, or the management of the organization. When an organization complies with the requirements mandated by government and/or governing bodies, then it is termed as 'regulatory compliance' which enables the organization to run in a legal and safe manner.

COMPLIANCE - AUDITS

Several organizations carry out compliance audits on a regular basis to avoid the potential consequences of non-compliance.
A compliance audit examines how well an organization adheres to compliance requirements. Some organizations use video surveillance to monitor compliance issues and audit recorded CCTV video footage from time to time for investigating and preventing compliance issues. Auditing CCTV provides actionable insights on the level of compliance within the organization.

AUTOMATED SOFTWARE – WHY THEY WILL NOT WORK IN ISOLATION

In the wake of the Christchurch shooting incident, several high-profile places of worship considered deploying gun detection technology. However, there are concerns about its efficacy, since it may not be able to detect all types of weapons, or the perpetrator could still create damage before being detected.
Similarly, automated systems like video analytics, AI/ML can only detect what they have been programmed for. What about the rest? Again, these technologies are prone to triggering huge amounts of false alarms.
Also, since the permutation combinations of exceptions can be vast and varied, it becomes almost impossible to automate every kind of exception. Facial recognition technology also raises ethical and privacy concerns, and has been found to produce inaccurate results, especially for certain ethnic groups.
Therefore, experts suggest that while automated technologies will continue to grow, human intervention and intelligence will still be necessary to verify alerts and ensure their efficacy.

"CCTV IS NOT ENOUGH – WE MAKE IT WORK FOR YOU"

While it is not being suggested that optimal usage of video surveillance can cure all issues, several issues of the following kind can be addressed by doing just a little 'more' with respect to making the optimal use of video surveillance systems:

- Recces/suspicious movements/activities

- Insider job/security lapses

- Bullying/violence/disputes

- False allegations and/or claims

- Sexual harassment and/or other kinds of abuse

- Unauthorized/unlawful activities/visitors

- Accidents/Causes of potential accidents

- Loss/fraud/theft

- Intrusions, especially by animals

- Inattentive staff (e.g. guard sleeping)

- Unruly staff/visitors/outside workers/security guards

- Parking issues

- Unclaimed/unattended objects

- Housekeeping issues

- Health and safety issues

- Issues with female staff or visitors

- Cameras/recorder malfunctions

So, what is the 'more' that needs to be done?

1) AUDIT CCTV VIDEO FOOTAGE DAILY AS A STANDARD OPERATING PROCEDURE

'Auditing' means 'seeing' what the cameras 'saw'. Auditing of CCTV footage should be done daily (continuous investigation) to identify potential issues and threats. Auditing is a dedicated and systematic process that helps address challenges related to live monitoring and alert-based systems. Auditing helps in evaluating analyzing incidents to improve existing policies, procedures, and processes. Concerned personnel should be trained to become CCTV video footage auditors, and the audit teams should be rotated to avoid complacency/collusion. Daily auditing of CCTV footage can also help in adhering to the principles of Kaizen and TQM for business improvement.

2) DOCUMENT AUDIT FINDINGS/INCIDENTS

Audit findings/incidents should be documented in a standardized template to find the root cause to prevent future recurrences. Historical data of such findings/incidents can reveal patterns that can help take better informed corrective and preventive action. If all IT companies report incidents in a standardized template, relevant authorities can derive business intelligence from the data and take action for the collective benefit of the IT sector.

3) ENSURE DISASTER RECOVERY OF CCTV VIDEO FOOTAGE – LIKE A 'BLACKBOX'.

CCTV video footage must be stored at multiple locations in order to ensure that even if the recorder is stolen, destroyed or tampered with the data is never lost. Further, any backed-up data must easily be searchable and retrievable; else, it is going to be a nightmare finding the relevant video.

4) DISPLAY DYNAMIC INFORMATION AT RELEVANT PLACES

Document and display details of information that is dynamic in nature in relevant areas. For example:

1. List of authorised staff.

2. List of authorized security personnel deployed at the IT company.

3. List of habitual offenders/suspects likely to visit the IT company's premises (a 'Watch out' list).

5) USE A POWERFUL NEW SIGNAGE

"WE AUDIT CCTV VIDEO FOOTAGE EVERYDAY".

One size, one color, one powerful message.
Across the nation.

DE-CENTRALIZED SURVEILLANCE + CENTRALIZED SURVEILLANCE = OPTIMAL RESULTS

Organizations with multiple locations struggle with centralized video surveillance due to infrastructure cost, internet bandwidth, and operator limitations. De-centralized surveillance offers higher accountability at each location and better situational awareness, leading to more chances of discovering exceptions.

CONCLUSION

“You see, but you do not observe” is a quote by Sherlock Holmes in A Scandal in Bohemia (1891, written by Sir Arthur Conan Doyle).
COM-SUR makes 'observation’ far effortless and effectual leading to superior results.

"Cameras don't lie" - but how will you know unless you 'see' what the cameras 'saw'?
Audit CCTV - why suffer!

Get award-winning COM-SUR now. Don't wait for things to go wrong!

Finally, allow us to present three important mantras that change the landscape of video surveillance:

1. Auditing is fundamental – everything else is peripheral.

2. Cameras have lenses – humans have eyes.

3. Let’s make cameras ‘accountable’.

