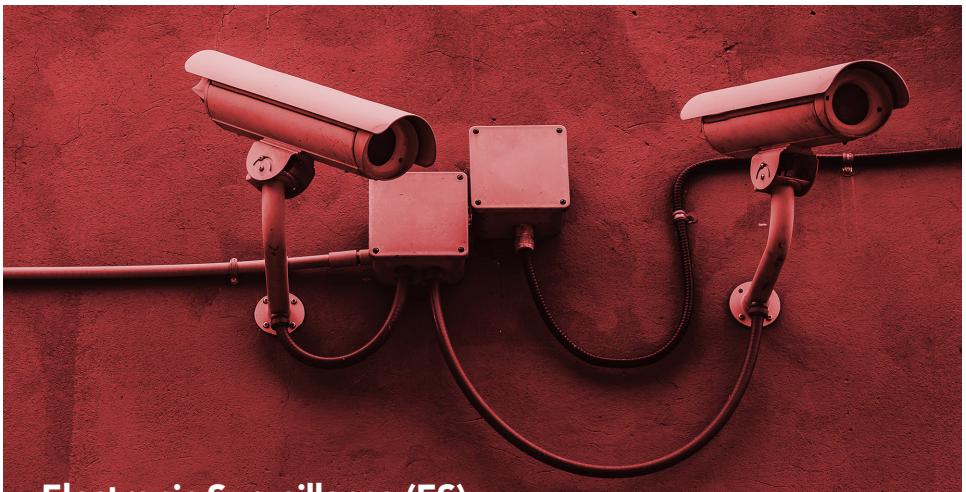
OMNIRISC
REDEFINING SECURITY

Security Newsletter

MAY 2018 I ISSUE 9



Electronic Surveillance (ES)

In this day and age, all aspects of our daily lives are watched over by the all-seeing eye of close circuit television cameras. They watch us at work, at home, in public places, on public transport, at entertainment venues, on roads, in lifts and in car parks. The list is seemingly endless.

Electronic surveillance systems are an important part of any physical security network. However, like an iceberg, only the tip (the camera) is usually visible, the remainder of the systems are hidden from view.

As with the other elements of physical security, we are likely to examine our requirements for electronic surveillance when we design and build a new facility, when we move into an already built structure, when we conduct a security audit or review or as a result of a major incident. As with all elements of physical security we need to be aware of the threats and risks that are expected and are being guarded against?

Our first consideration is what is the risk and what are we trying to achieve with our ES system design and placement? Are we focusing on crime prevention, public/crowd safety, traffic monitoring, staff conduct, external perimeter monitoring, access control, inventory control or a variety of combinations of these?

Lights Cameras Action

An electronic surveillance system consists of:

- Cameras
- Wired or Unwired image transmission
- Image reception, monitoring and recording
- Image storage and retrieval and investigation
- Incident response and observation.

The effective combination of these various components will produce an efficient and cost- effective electronic surveillance system that will enhance your physical security network.

Lighting

The system design needs to take into account the daytime and nighttime lighting conditions chosen for camera placement. Camera efficiency is affected by direct sunlight, shade and shadow. These areas of concern need to be mitigated by protecting the cameras or by enhancing the nighttime lighting conditions so that the cameras operate to maximum efficiency. Day/night, lowlight or infrared cameras may have to be used to obtain this.

Cameras

Once we identify what we want to achieve, we can select the best type and style of cameras and camera lenses for the job. These can be both video or still picture capture and include:

- Dome Cameras
- Bullet Cameras
- C-mount Cameras
- Day/Night Cameras
- PTZ Cameras [Pan Tilt Zoom]
- Infrared Cameras

Once we have selected the most suitable camera combination for our requirements our next consideration is positioning and lighting.

OMNIRISC SECURITY SERVICE (MACAO) LTD. 26 Avenida De Marciano Baptista, Chong Fok Comercial Centre, 12/H, Macau
Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com

Where to position them for the best coverage and effect will depend on the overall aim of the particular camera. Is it placed on a perimeter fence or wall? The building exterior or internally? Is it used for pedestrian or vehicle access control? or for vehicle number plate/driver identification? For facial identification with access control or for staff observation?

Wired/Unwired image transmission

Once the various cameras have been chosen and positioned their image capture/signal needs to be transmitted back to a central point. This is usually a security control center or in smaller operations a computer monitor. This transmission can be achieved by fixed wiring ground buried or internally buried in the building, by an externally fixed cable or by a wireless transfer. All three have vulnerabilities and cost implications that must be considered.

Action

We have considered what we want the surveillance system to achieve, chosen the best positions for the cameras, have taken the ambient lighting conditions into consideration, decided whether to have video or still picture capture, chosen the best camera and lens combination and connected them to somewhere! So, what happens next? Where is the rest of the Iceberg?

What can OMNIRISC do to help you:

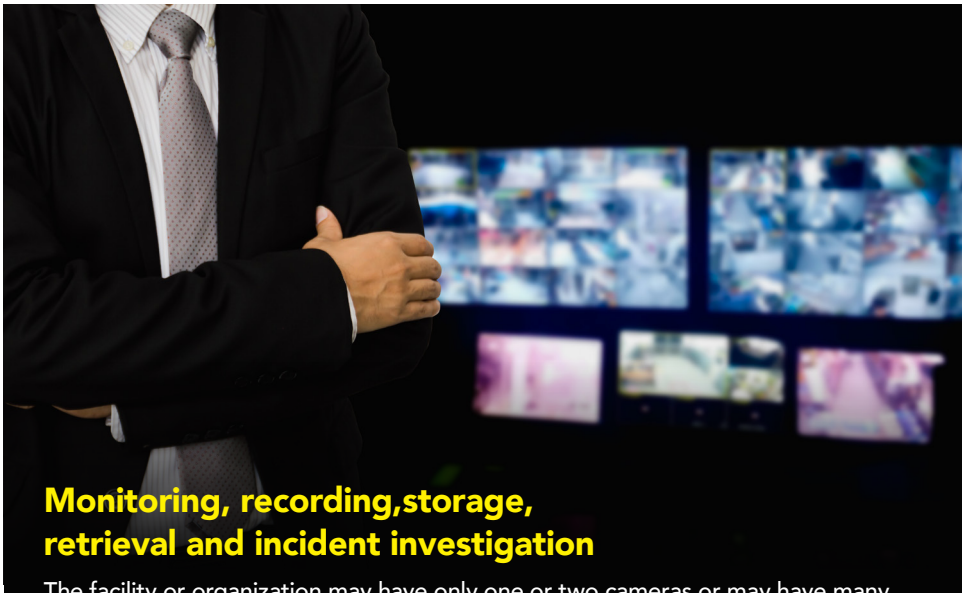
We provide bespoke consultations for businesses and organizations on security and on various levels of vulnerability and risk assessments.

About the Author

James Langton, is an advisor to "OMNIRISC" and a specialist in physical security auditing.

The article is designed and edited by Ekraj Rai.

OMNIRISC
REDEFINING SECURITY



Monitoring, recording,storage, retrieval and incident investigation

The facility or organization may have only one or two cameras or may have many more. In its simplest form these may terminate on a computer or may terminate in banks of monitors in an operations center. These may be monitored live 24/7 or just recorded for later playback where necessary.

There are many systems that allow for storage of recorded data for a variety of periods. How long you need to store surveillance data depends very much on your operational needs. Stored data is an extremely useful investigative tool for your own investigations and for those of the authorities.

In the aftermath of the incident at the Mandalay Bay hotel and casino in October 2017, the CCTV footage was used extensively by the Las Vegas authorities to aid the investigation of the tragedy.

Incident response and observation.

An effective surveillance system must be combined with incident response and incident monitoring. Unfortunately, this is usually only available where live monitoring takes place.

Facilities standing operating procedures (SOPs) should cover what to do regarding incident response. While this is ongoing the monitoring team can watch the incident unfold in real time and pass critical intelligence to first responders. This is vital to ensuring an effective response

Surveillance system audit

Finally let's look at the problem from the angle of conducting a surveillance system audit:

- What risks/threats are being considered?
- What is the ESS trying to achieve, what are its aims?
- When was the last ESS review conducted?
- What is the security manager/teams' opinion of the quality and effectiveness of the ESS?
- Are the camera positions correct and achieving that desired outcome?
- Is the lighting sufficient/deficient?
- Are the selected cameras fit-for-purpose?
- Is the transmission method wired or wireless? Are there any vulnerabilities?
- Where do the transmissions terminate?
- Are they monitored live or just recorded?
- How many monitors does the operator have to observe?
- What incident SOPs are in place?
- What procedures are in place to respond to faulty cameras?
- Where is the surveillance data stored?
- How long is it stored for?
  How secure is it?

An effective electronic surveillance system is a vital part of the overall physical security network that deters, detects, delays and records unwanted actions. It allows human guarding resources to be better used.

In subsequent issues we will continue to examine further elements of physical security and security auditing such as human guarding and security control and management.

Office: +853 28558964 Email: info@omnirisc.com
www.omnirisc.com