How to professionally specify your IP camera network

The past decade has seen camera surveillance technology rapidly evolving. Of significance was the much-anticipated shift from analogue closed circuit television (CCTV) to Internet protocol (IP)-based systems. It is now widely accepted that the benefits of IP far outweigh analogue, but the selection and specify of an IP surveillance system now presents new challenges.

Marc van Jaarsveldt, consultant for The Surveillance Factory, a video surveillance system-integrator, says that there are some important aspects to keep in mind when using IP-based technology: "It is not simply purchasing a system, but more about understanding what system and cameras you need, the network design, cabling and viewing requirements. There are many pitfalls to avoid and these could prove costly should you not address the basics adequately."

Van Jaarsveldt offers us the following do's and don'ts when designing an IP video surveillance system.

Do's:

- Prepare a detailed site audit report of the site before installing any cameras
- Always understand the security requirements and the risk environment
- Consider dark screen monitoring for event-based monitoring to increase operator vigilance
- Offer offsite monitoring if budget is available
- Agree on upfront SLA's (Service Level Agreements) to ensure your surveillance system is always running optimally. This should include software assurance/upgrade packages from the VMS provider
- Cover basic, but important, maintenance elements such as cleaning lenses and focusing cameras routinely
- Specify the hardware required properly. This includes, viewing stations, servers, NVRs's, storage, network infrastructure and network cables
- Consider doing a shoot-out to compare products
- Involve a consultant if the project is big enough so you can gain value form their expertise and neutral brand position

- Specify workstations and separate the recording system from the display machines
- Lighting is very important because without it, true colour cannot be seen, identification cannot occur and you will lose forensic information
- Consider surge protection on switches and outdoor cameras as these can neutralize the damaging effects of power surges on PoE
- For outdoor cameras, ensure you have vandal-proof cable routes and they are sealed or placed in Bosal/Kopex conduit, for example.
- Be cautious when using PTZ cameras. They are suitable for monitoring environments with vigilant operators and offer little value as general overview cameras. Automatic patrolling software offers very little by way of enhancing security.
- Make note, cameras to identify faces need to be extremely close to the target, at face height, have very good lighting and need to have high-resolution sensors

Don'ts:

- Don't do covert surveillance. Surveillance prevents theft by being overt and acting as a deterrent and it is often a waste of money if the perpetrators figure out that the camera is either fake or hidden
- Restrict company access to the cameras and don't let the IT department manage the surveillance system. They are not generally surveillance and security specialists
- Less is often more. Consider the design and number of cameras required. A good consultant will not suggest you have a camera in every corner of the room – they will suggest a strategic layout where each camera is purposed properly.
- Don't be afraid to ask questions to the installer. Security jargon can be hard to follow.
- Try and avoid wireless equipment to stream high-definition video streams. Wifi is often unreliable and unpredictable, especially indoors. Point to point wireless links can work well outdoors if they are dedicated, and specified properly

For more information or assistance, contact The Surveillance Factory on 086 111 3635 or visit www.sfactory.co.za.