Video
Surveillance.com

Information Technology
Guide to Video Surveillance

Table of Contents

Introduction

IT departments are becoming increasingly responsible for the research, installation, and management of video surveillance systems. Creating a process for handing data, archiving data, and designing a system that minimizes the impact on your bandwidth will take a large amount of planning.

A 2013 joint study by Axis Communications and ESG found that "Although video surveillance has traditionally been a task handled by facilities or physical security groups, IT departments are increasingly involved as these implementations continue to evolve from analog cameras with proprietary DVRs to IP-based solutions with networked storage options."[1]

3 Challenges for IT

The three main challenges that IT departments face when managing surveillance systems, according to the Axis/ESG study, are:

- Search & retrieval of archive footage
- The impact on network bandwidth
- Difficulty managing the growing volume of data

This guide will highlight the questions you need to ask as you take over the management of a surveillance system; while the specific answers will depend on your equipment and network, having the right questions to ask will get your project off to a good start.

Network security is the key concern of many IT departments, but you can create a secure system that only allows access to the users of your choice, with the level of permissions you assign them.

While many IT departments have the technical and networking know-how to competently manage an existing system, they often lack expertise in physical security and other issues that affect image quality. By leveraging the expertise of trusted security partners, IT directors can help ensure their facilities are protected, and that users across the organization can easily view high quality video to better manage operations.

---

[1] Source: Axis Communications & Enterprise Strategy Group (ESG) Research Report, Video Surveillance: Now on IT's Watch, December 2013.

What if You Inherit a System?

This is an extremely common position for an IT department to be in – your business can no longer manage the system the way it has been, so now it's on your team. How can you make sure this transition goes smoothly?

Key Questions to Ask

It can seem overwhelming to take over management of a surveillance system, but asking the right questions from the beginning will get you off to a good start:

- Have you taken inventory of all parts on the system?
- How will you centralize everything if it's in multiple buildings or systems?
- How old is the system? How functional is it? What is the system's health?
- What are the requirements of the system?
- Who managed the system before?
- How was user access & back-end access managed?
- How is data pulled from the system?
- Was an upgrade plan ever created?

Being asked to manage or fix a surveillance system your team was not responsible for designing and installing is often the position an outsourced or 3rd party IT department finds itself in. Commonly only called in when there is a problem, it is especially important that you get access to all documentation.

Checking the Health of your System

You will want to verify the health of your surveillance system to ensure it is working properly. Pay special attention to how your system is recording:

- Is the timestamp correct?
- Are motion detection settings correct?
- Is user & system access secure?

Getting a Handle on the Project

Once you've gathered the basic information about the size and scope of your new system, it's time to gather more details. Having this information before you purchase any new equipment or plan upgrades will help streamline the process. Gathering this information before talking with a surveillance partner will also make it easier for them to fully understand your system:

- Have all IP address information for your equipment
- Have all current username and password information
- Verify the health of your system and your network

Designing a Video Surveillance System

If you aren't already familiar with surveillance system design, each system is made up of some combination of these basic components:

- Surveillance cameras
- Video management software (VMS)
- A server or network video recorder (NVR)
- Networking equipment, including PoE switches & wireless antennas
- Long-term storage

While the specific features of your equipment are important, you should always clarify the goals of your video surveillance system before ever comparing products. This will help you identify the right equipment for your surveillance needs from the beginning.

General IT Responsibilities

Each business and IT department will handle the design, implementation, and management of a surveillance system differently. But some of your responsibilities could include:

- Server configuration & setup
- Setting up remote access & admin access
- Supporting the equipment & software
- Handling requests for video file downloads & backup
- Monitoring system performance & management
- Installing cameras & equipment
- Upgrading cameras & equipment
- Integrating the surveillance system with other systems

Common Design Mistakes

While the system may seem like a simple thing to design, it is easy to make mistakes if you aren't familiar with the equipment. After years of working in the surveillance technology industry, the most common mistakes we've seen all stem from a lack of knowledge about the products and not having a clear plan:

- Incorrect camera resolution & lens choice
- Purchasing equipment without considering future system expansion
- Not checking the health of the network before installation
- Installing the system without adequate knowledge
- Decentralized system management & ownership

Tips for Successful System Design

The best video surveillance system is one customized and designed for your security needs. As your team moves forward, keep these four categories in mind: system stability, data retention, network security, and physical data security.

Working with an experienced surveillance system integrator can help ensure your system is designed to meet both your current and future requirements.

Evaluating Surveillance Cameras

You cannot choose the right camera if you haven't thought through its purpose. When looking for cameras, consider:

- What is your intended role for the camera?
- What field of view & image quality do you require?
- What special features do you want?
- Where will you mount the camera & what power options do you have there?
- What is the lighting like at that location?
- Does that camera location require specialized housing to protect it?

An experienced surveillance partner will recognize these mistakes before you ever deploy your equipment and help walk you through the process of planning a successful system.

Evaluating Software & Servers

A benefit of video management software is that it will be compatible with most of the equipment on your current server, a NVR you already use, or a server you build specifically for managing the surveillance system. This will allow you to evaluate the VMS options primarily on features, rather than worry about compatibility.

When looking at your current server, or the possibility of building a new one, pay special attention to the CPU and memory. Video recording and management draw heavily on a server's CPU and memory, so make sure you allocate more budget to these components.

In addition, you should consider:

- How many cameras you need
- What your system performance goals are
- Determine the level of operation & complexity you want
- Decide on the number of users & user access permissions
- Lay out your data storage requirements (onboard RAID, NAS, SAN, etc.)

Future-proofing a System

When designing and purchasing your video surveillance system, plan for eventual system growth. At some point you'll want to add new cameras or equipment to the system; planning for this eventuality from the beginning will make this process easier. The idea of "future-proofing" a system will be explored in-depth later in this guide, but for now you can ask think about these ideas:

- VMS + server scales better than a NVR (due to more flexible channel licensing options)
- Storage is fairly easy to expand or upgrade
- IP cameras scale better than analog CCTV (since they are networked rather than directly attached to a DVR)

Surveillance System Management

There are two central problems you must answer to smoothly transition the management of a surveillance system to your IT department. These will be expanded in a later section, but they are:

- Decide from the beginning who will own & manage the system
- Create a network implementation plan & parameters before starting the work

What about Industry Codes & Regulations?

Many industries have strict requirements for security that your business must meet to obtain or retain your business license. These laws and requirements can be difficult to navigate, especially if you are not familiar with surveillance technology. Partnering with an experienced surveillance company that has the tools necessary to meet strict codes will make this process easier for your business.

For example, the quickly changing landscape of legalized marijuana in several states has created strict security requirements on all businesses applying for operating licenses. Each state also has strict requirements for camera resolution, placement, restricting system access, how the time and date stamps can be formatted, and more.

- Oregon: 1 hour minimum battery backup; must record 24/7, minimum 30 days storage
- Washington: 45 day minimum storage
- Colorado: 40 day minimum storage

Other Regulations

- **Hazardous Materials** - Federal regulations for companies that handle restricted chemicals and materials must secure and monitor all building entrances and exits, with safety plans in place for any unauthorized access attempts.
- **Public Transit** - Public transit authorities passed surveillance requirements for the city of Stockholm in 2005, including 24-hour recording and vandal-proof cameras in both the driver's area and the passenger area.
- **Financial** - Financial institutions can also face strict requirements for storing video, from one week to several years.

If your business's surveillance system cannot meet these strict requirements, or the system implementation is delayed, your business license could be revoked or denied. Pay close attention to such requirements when researching and designing your system, and clearly communicate all security requirements to your surveillance partner.

Bandwidth & Networking Considerations

Your surveillance system does not have to be a drain on your bandwidth or network resources with proper management, a good system design, and modern equipment.

Specifically, you may want to:

• Limit system monitoring to essential personnel

• Upgrade your cameras to the latest compression technology

• Evaluate each camera to adjust resolution & FPS for optimal performance

You can, and should, separate video and data traffic from the rest of your organization's network using a separate LAN or VLAN. Most high performance servers and NVRs are designed with dual NIC, so admins can segregate inbound video streams from cameras from the network where users view those streams on their workstations.

What if Your Camera Network is Slow?

If your surveillance system performance is sluggish, try these possible solutions:

• **Look at video compression** – Your camera will likely offer more than one compression format, and you can set each one to a different level to help reduce the size of the video stream.

• **Also look at video resolution** – Higher resolution images require more bandwidth, so record and stream video in an appropriate resolution for your needs (you can stream video at a lower resolution and save at full resolution).

• **Video frames per second (FPS)** – You can also have two different settings for streaming and saving – stream the live preview with low FPS but save at faster FPS.

• **"Noise" from poor quality night video** – This generates false motion alerts which trigger frequent recording, as well as greatly increases the bitrate of the video stream (noise is difficult for compression algorithms), but camera settings can be adjusted to reduce this problem

• **Your network may also be an issue** – Ideally the network should be gigabit or 10gig speeds for optimal video viewing, otherwise video traffic will slow it down.

Networking FAQ

Q: Can I restrict access to specific IP addresses? Or to a few users?

A: *It is highly recommended that you restrict access to the system, and some industries even require this. In general, all surveillance equipment supports the creation of user accounts; by limiting who you create user accounts for, you can limit who has access to your system. You can also restrict access by IP, which is often done through the firewall or your modem/router.*

Q: How will remote access work with a firewall?

A: *You'll typically need to set up port forwarding for remote access through a firewall. Some systems have built-in VPN clients that auto-connect through a firewall using a secure VPN tunnel. Please note, however, that remote access may not work if your organization has a very strict firewall that does not allow any outside access.*

Q: Can users remotely change the settings on the server?

A: *No, unless you have set up their user accounts to give them this access. When you set up individual user accounts you get to assign their permissions.*

Q: Can I set up the system on its own private network?

A: *Yes! You'll want to use a dual NIC and separate wiring and switches when you install the system, but this is the recommended solution.*

Q: Can the system work with the server and cameras on a different subnet?

A: *Yes, the system will work set up this way. You can use dual NIC or VPN tunnels.*

Q: Can the system work without a DHCP controller?

A: *Yes, but make sure to set the static IP addresses before the system is installed, as some cameras require DHCP to initialize correctly the first time.*

Q: Does the server require authentication?

A: *It can – this will depend on how you've set up the system. This is recommended for almost every surveillance system, because it makes the system more secure.*

Video Storage & Data Retention

While the amount and type of storage your surveillance system will need greatly depends on how your system is used, storage is a key component of every system. Purchasing the correct type and amount of storage, and setting it up correctly from the beginning will save you time and money.

Video Storage Options

Depending on the number of camera you have, how long you want to keep the files, and how secure you need the system to be, you can choose from:

VMS installed on a NVR or hard drives in a server
This is the basic system setup, giving you flexibility in system size and storage options.

On-camera, or Edge recording
Many IP cameras include slots for memory cards, or have built-in storage. Because storage space is limited this is not recommended as the primary storage on most systems, but is best utilized as a fail-safe if the camera ever loses connection to your network.

NAS or cloud storage
Cloud storage is growing in popularity, but it is just one type of off-site storage. Whether you store archived video on the cloud, a second server, Network Attached Storage, or an off-site server, setting up automatic data backup is recommended. Archival is particularly important for long-term storage and for extremely important recorded events. Real-time off-site or cloud storage requires very fast upstream connection.

Storage FAQ

Answering these questions, or working with a surveillance partner, will help you when designing a system:

Q: How long does the data need to be stored?

A: *This may depend on your industry or business standards. As a general rule, unless you have requirements that state otherwise, we recommend a minimum of 30 days.*

Q: How much hard drive (HDD) storage space do I need?

A: *This will also depend on any requirements you need to meet, and how you are using the system. If you record 24/7 you will need significantly more space than if you only record on motion during non-business hours.*

Q: What type of hard drive should I use?

A: *Traditional hard drives are still the best option, and they are quickly dropping in price even as the size increases.*

It is important to select the correct grade of disks due to the intensive nature of surveillance systems write activities. Professional-quality HDD are recommended, and some manufacturers also offer "surveillance grade" and "server-rated" drives.

Solid state drives (SSD) are a more expensive and newer technology, one that has not been tested long-term in a surveillance setting. Because of this, you may want to only use them to run your software programs or operating systems.

Q: Do I need a RAID?

A: *A RAID (redundant array of independent disks) setup will help reduce your risk of losing important data if a hard drive fails. While it will take some time to configure a RAID, it is highly recommended that every professional-quality system do this to protect your data.*

Data & Network Security

Installing a surveillance system shouldn't make your network less secure. Researching and planning your system before implementation, working with a skilled surveillance partner if needed, and utilizing all security settings during installation will help keep you safe from breaches, hacks, or network attacks.

Camera & Server Security

When installing your system, start with the cameras – are they in a location that makes them hard to access? Not only will this protect them from theft, vandalism, or tampering, it will make it harder for someone to use the cameras as a physical access point into your network. You should:

- Install the cameras high up on a wall or in the ceiling
- Run cables through the walls or ceiling
- Use managed switches
- Use a closed network with no DHCP available

- Enable camera tampering alerts, if available
- Put your cameras on a segregated network
- Make sure all switches are hidden from sight

In addition, you should always lock and password protect your WiFi. You can also lock it to a specific MAC address to restrict access. You should also evaluate the security of your server room. Is it locked? Do you restrict access? Using an access control system and installing a camera in the server room will help you log and track all entry into the room.

User Management

Integrating your system with a corporate Active Directory can increase the security of your server. This is recommended as the way you organize all users who have access to the system, and can make it easy to integrate with other software on your network. If you do not have an Active Directory, you will need to actively manage individual user accounts and activity.

Best Practices for System Security

To ensure the security of your network, proactively take steps to manage all users. These tasks can help with your system management and security:

- Change passwords on all equipment from the factory default
- Limit the number of users who have access to the network
- Place your system behind a firewall & on its own LAN or VLAN
- Install equipment to monitor your server room
- Log all access to the system & server room
- Consistently save & backup any sensitive data
- Run regular health checks on your system

Installing Your System

There are generally two ways organizations commission a new surveillance system – managed installation, and self installation. Both options have benefits, and which route you choose will depend on the skills in your department, project timeline, and budget.

Managed (3rd Party) Installation

Managed installation is when you pay a security company, electrician, or other technician to install the system for you. The installer will handle all system installation and setup on-site.

Benefits of Managed Installation

- **Easier on your team** – you will not be required to become product & technology experts overnight
- **Faster setup** – an expert who has handled hundreds of systems can work faster

When to Consider Managed Installation

You may want to go with a managed installation if your team is on a tight deadline (assuming the company can meet your install date) or you need to meet strict and specific codes.

Self Installation

If your team has hands-on technical knowledge and the ability to run network cable, you may want to install the surveillance system yourself. But this doesn't mean you can't have a surveillance partner – look for a partner that offers "Supported Self Installation," where they provide remote guidance and support during the design and installation process so you're not left on your own.

Benefits of Self Installation

- **Lower cost** – using your own department personnel can save you thousands
- **Better product knowledge** – it can be helpful for staff supporting the system to have hands-on experience during setup.
- **Complete Documentation** – by handling system installation, your organization controls the system documentation and can insure it's written to your internal standards.
- **Save time on setup** – your surveillance company can work with you to ship the system so you won't have to work around an on-site technician's schedule.
- **Remote assistance when you need it** – by using an IP system you make it easy for a remote partner to log into your system and help with setup issues

The Importance of Bench Testing

Bench testing is recommended for all surveillance systems, but will be especially important if you are installing the system yourself or inherited the system. You may be tempted to skip this step, especially if you are crunched for time, but bench testing gives you important access to the equipment.

You can familiarize yourself with the user interface, set up connections on wireless systems, and identify any problems with equipment or network connections before everything is installed and harder to fix.

When to Consider Supported Self Installation

In our experience, most IT departments have the technical skills to configure and install a surveillance system with our guidance.

This is a great option for those organizations looking to reduce both initial project cost and total cost of ownership, or who just like tighter control over systems installed in their facilities.

Guide to Ongoing System Maintenance

Being proactive in your system maintenance will save you from experiencing larger problems in the future. The key is to set up regular maintenance steps so you aren't taken unaware when a problem occurs.

While the specific tasks will vary, keep these tasks in mind when creating a video surveillance maintenance plan.

Daily Maintenance

- Check the power on your server
- Check the connectivity & feeds of each camera
- Check the connectivity on all other equipment on your network

Weekly Maintenance

- Run all Windows updates
- Reboot your server & ensure it restarted successfully
- Run a full virus/malware scan & respond to any threats
- Check for any video footage that needs to be exported

Monthly Maintenance

- Check for any change in the surveillance environment
- Check all motion detection settings & update as needed
- Check for program & firmware upgrades and install them
- Manage your system's security
    - Remove users who should no longer have access
    - Change system passwords
    - Grant access to new users
- Do a RAID health check

Bi-annual Maintenance

- Run a full system health check
- Respond to any issues that come up, paying specific attention to
    - HDD defrag
    - RAM scan

Planning for System Expansion & Upgrades

It is inevitable that at some point you will want to expand or upgrade the system – planning for this now will help when you go to upgrade the system in the future. There are many reasons to expand or upgrade a system, including:

- Making the switch from analog to IP
- You've added new buildings to your campus
- You moved to a larger building
- You want to standardize equipment on the system
- There are new requirements for your system

Making the Move to IP

The most common upgrade request we see is the move toward IP systems. Analog, or CCTV, technology has been the standard in video surveillance for over 30 years, but the larger number of camera and software features available with IP equipment is pushing many businesses to switch.

But this process does not have to be done all at once – many organizations cannot afford to replace an entire surveillance system, or they still have analog cameras that work well for their needs. In this case, you can use specialized equipment like video encoders and hybrid NVRs to add IP cameras to your system over time.

If you are planning to take the phased upgrade route, remember to think through the entire process before you start. Knowing when your equipment will reach its end of life will make the transition faster and easier.

What to Consider when Upgrading

Keep these things in mind when creating a system upgrade plan:

- Number of analog cameras you keep vs. new IP cameras
- Is the current resolution of each camera sufficient?
- Do you have the correct VMS licensing?

When is it Time to Start Fresh?

Sometimes, however, the phased process just won't work for your system. This could happen if:

- There are too many issues, driving up the cost of repairs as well as upgrades
- Poor documentation of the current system
- Very old or obsolete equipment that needs to be replaced soon anyway

You may also be facing new system requirements, updated licensing codes, or equipment standardization that your old equipment will struggle to meet. In this case it may be faster and easier to design a new system with these goals in mind from the beginning.

Your Surveillance System Checklist

Video surveillance systems are complex systems, but with proper planning and management they do not need to create undue pressure on your department. You'll get the most value by planning properly from the beginning, so ask yourself these questions.

IT Department Responsibilities

☑ Have you figured out what responsibilities will fall on your department?

☑ Who will manage researching new equipment?

☑ Who will design your system?

System Design

☑ How will you manage the bandwidth impact?

☑ How will you store & back up data?

☑ How will you secure your system from digital & physical attacks?

☑ Who will create & manage user profiles?

☑ How will you manage a separate LAN and the firewall?

☑ How will you install the system?

System Management

☑ Do you have an upgrade & expansion plan?

☑ Do you have a plan for equipment failure?

☑ Who will take on the system maintenance tasks?

What Next?

This guide has asked you a lot of questions. You may not have all the answers right now, but thinking about and answering these questions as you design, install, and manage your surveillance system will make the process easier on your team.

As an industry-leading security integrator who has helped thousands of organizations in more than 60 countries, VideoSurveillance.com is here to help your business succeed.

With our Supported Self Installation service, our company is uniquely positioned to leverage the skills in your IT department to bring you greater savings and service.

Give us a call today and we'll partner with you to design and implement the solution necessary to secure and manage your business.