



Our View of Security Video Surveillance “Do’s and Don’ts”

presented by Nicholas A. Smith, WTW Security Risk

Video Surveillance is an important component of many private sector, public service agency, and non-profit organization security postures and programs

Camera systems, when properly designed, installed, maintained, and utilized, can serve to effectively aid you in deterring, identifying, and alerting to unwanted scenarios to include misconduct and theft. Follow our Do’s and Don’ts below to assure a best practice program which contributes favorably to your organization’s physical security stance.

Do:

- ✓ Determine a video surveillance strategy for your organization (goals; purpose, expectations) prior to engaging a vendor and installing systems:
 - Are the cameras intended to deter misconduct or crime or are they aimed at investigative outcomes?
 - Do you expect to “monitor” camera images or is the video data intended more for follow-up investigative purposes (IE: detection of aberrant behavior, security investigations, Worker’s Comp cases)?
 - Think about your sector and unique needs. For example, the Gaming Industry, Hospital sector, Real Estate, and Retail each have different video requirements and goals. As well, a Corporate Office or a Warehouse Distribution Center possesses specific risks which cameras can help mitigate.
-



Do:

- ✓ If camera systems are already in existence across your site or real estate portfolio, survey and assess them in detail. Capture make, model, camera device locations et al so that you may understand the current embedded base of “CCTV”.

- ✓ Carefully think about whom in your organization should have access to the system and who will administer it. Restrict system access and delete users immediately when they separate.

- ✓ Consider implementing a video surveillance Policy. Consult with Legal, outside Counsel, HR, or others:
 - Prohibit covert cameras in workplace, absent special Legal approval in unique investigative circumstances
 - Make clear that cameras are not to intrude upon anyone’s reasonable expectation of privacy
 - The best camera system posture for most organizations includes covering points of ingress into the workspace, loading docks, Computer/LAN Rooms, Reception Area, and down corridors.

- ✓ Partner with a trusted security integrator to design, install, and service your system:
 - Learn the current state of the security industry’s video surveillance system technologies before choosing a camera system.
 - Consider: Digital, IP-based, Cloud, DVRs or no-DVRs, Remote Viewing capability.

- ✓ Consider posting appropriate signage, if necessary.(IE: “Notice – Area Under Video Surveillance”; “Cameras Not Monitored”).



Don't:

-
- ✓ Put “dummy” cameras up. Deploying inoperable cameras is highly discouraged. They give a false sense of security and may lead to liability concerns.
-
- ✓ Deploy cameras absent a strategy. This approach results in excessive spend, poor security performance and return on investment, and even misuse of video surveillance systems.
-
- ✓ Allow decentralized camera systems to pop up across your organization.
-
- ✓ Overlook the network considerations. Are there bandwidth concerns? Should Security have its own separate network?
-
- ✓ Fail to secure your video head-end. Ensure that it resides within the LAN Room, an IDF closet, or other secure location.
-
- ✓ Install expensive Pan/Tilt/Zoom cameras when Fixed cameras will suffice. Especially when you have no security guard or security control center to monitor the cameras.
-
- ✓ Find yourself without a video system preventative maintenance agreement with your vendor. All system devices ought to be tested regularly.
-
- ✓ Forget to consider privacy laws and regulations.
-
- ✓ If in a tenant or commercial mixed-use environment, neglect aligning your camera systems with the Landlord's video surveillance programs.
-
- ✓ Install cameras at pools, hot tubs, fitness centers, etc., without first prudently establishing correct (and Legal-approved) signage and monitoring plans.
-

Video surveillance can add tremendous value to your organization's security toolkit. Follow the suggestions, our Do's and Don'ts, in order to ensure a sophisticated and well-thought out approach to the use of cameras. We remain available to assist you directly.



Nicholas A Smith, Jr., CPP

(610) 651-7704

Nicholas.A.Smith@WillisTowersWatson.com

Nick's experience includes serving as Global Physical Security Director for American International Group and as a Regional Security Attaché at U.S. Embassy Athens, Greece

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas – the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.



willistowerswatson.com |  |  |  |  | 2 / 2 |  |  | 