MURRAY ASSOCIATES

SPYCAM DETECTION TRAINING

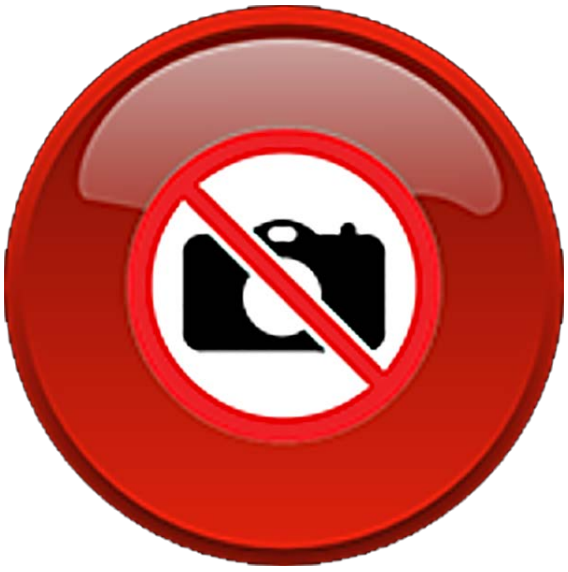


TABLE OF CONTENTS

About the Course

This course provides organizations with the basic security training necessary to mitigate video voyeurism risk for their employees and visitors. In turn, this helps protect organizations against expensive law suits and damaging publicity.

Every organization has inviting targets for video voyeurs: restrooms, showers, locker rooms, changing booths, tanning booths, etc., also called Expectation of Privacy (EoP) areas. Covertly recording personal activities in these areas has never been cheaper or easier. This has resulted in a workplace video voyeurism problem of epidemic proportions.

The security, financial, and emotional consequences of video voyeurism are very serious. Not addressing this problem proactively is risky. Considering the close ties with legal issues like foreseeability and sexual harassment in the workplace, the risk is not worth taking.

The course is primarily useful for:

- security directors,
- facilities managers,
- store managers,
- security officers,
- landlords,
- targets of activist groups,
- and real estate management companies.

Learning how to recognize and detect spy cameras is also a valuable skill for:

- law enforcement personnel,
- security management students,
- and the general public wishing to protect themselves against video voyeurism.

Course Syllabus

I. Introduction
A discussion of the four main motives which prompt surreptitious workplace recording. Emphasis is on the video voyeurism motive in Expectation of Privacy (EoP) areas and the reasons a proactive response is important.

II. Laws
A brief review of the laws governing covert recording.

III. Strategy
How does an organization deter unauthorized recordings? Written policy, due diligence inspections, and an awareness of who has the time and opportunity to plant covert recording devices are discussed.

IV. Spycam Identification
In this section we review portable vs. in situ cameras; what cameras do with what they see; and how voyeurs view what their cameras see. Video clips show the various types of spycams one is likely to find in EoP areas, thus making identification during an inspection easier.

V. How to see through black plastic enclosures.

VI. Inspection & Recap
The ABC's of how to conduct an EoP area inspection to detect spycams.

VII. How to Handle a Find
You found something! Now, what do you do?

VIII. Quiz
Take the quiz, pass the course, print your certificate.

Introduction

Welcome to Spycam Detection. Here you will learn about video voyeurism in the workplace, and your organization's strategy for preventing it. You will also learn about spycam technology, identification, detection and the steps to take if a spy cam is discovered.

My name is Kevin Murray. I'm a counterespionage specialist. Your organization has asked me to provide you with these skills because you are in a unique position to keep the workplace safe. Some of these skills will also help you to protect your own personal privacy, in places like hotel rooms, and public restrooms.

The video portion of this training is divided into the chapters you will see on the left side of your screen as you progress. You can start and stop a chapter at any time, as well as review previous chapters. You cannot skip forward, however.

The written course text file provides checklists, links, policies, and detailed information not shown in the video. Please download it and review it.

There is a short quiz at the end of this training, as well as a Certificate of Completion.

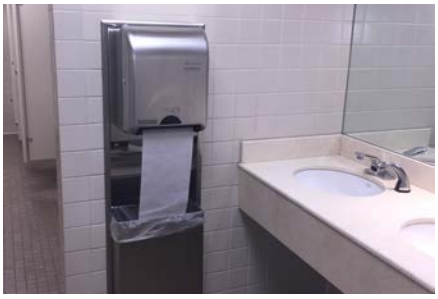
WHO IS AT RISK?
Almost all organizations are vulnerable to electronic voyeurism. Any place offering employees, customers, and visitors a space where personal privacy is expected is at risk. We call these ***Expectation of Privacy*** areas, or **EoP** for short. Very few organizations are exempt from this threat. If you have a restroom, you have a risk.

Dozens of stories appear in the news every week about spycams being placed in EoP areas. Locations include: toilets, locker-rooms, showers, changing rooms, maternity rooms, tanning salons, doctors' offices, under desks, gyms, swimming pools, saunas, yoga and exercise rooms.

VIDEO
VOYEURISM

If you have a restroom, you have a risk.



It is important to understand that news reports represent a minute subset of the problem. News reports *only* identify the voyeurs who have been caught and arrested. These are the *failed* attempts at voyeurism. They are the tip of the iceberg. The vast majority of electronic voyeurs get away with it.

A recent Google search using the word "voyeurism" and the subheading "news" returned about 31,400 entries; 43 screens worth of links in just the previous month. Extrapolating from these numbers it becomes clear the problem is rampant.

Workplace voyeurism is becoming a "foreseeable" issue; a legal term, loosely meaning, "You know this is a problem. If you don't do something about it, you will be held responsible for the next incident."

Given this level of risk, potential legal expense, and embarrassing publicity, inspecting EoP areas for covert recording devices has become an important security function.

Technical Surveillance Countermeasures (TSCM) inspections – a search for bugs, wiretaps and optical surveillance devices – are routinely conducted by organizations to combat espionage. Often they include a few EoP areas near the executive suite and boardroom. Unfortunately, EoP areas are found everywhere in large organizations and subsidiary locations.

Most businesses offer restroom facilities. Every location has some level of risk. Imagine, Starbucks with 22,000 stores and 44,000 publicly available restrooms. Obviously, hiring a professional TSCM inspection team to conduct inspections is not cost-effective.

On the plus side, conducting inspections for spy cameras in EoP areas can be conducted by any on-site manager. These inspections do not require the same level of expertise and specialized instrumentation used in executive suite searches. With training, one can find all but the most well-hidden video surveillance devices in EoP areas. This training program will prepare you to conduct an inspection.

WHY TAKE ACTION?

- To protect people's privacy.
- To reduce the voyeur's window-of-opportunity.
- To show due diligence and reduce monetary exposure should an incident occur.
- To avoid bad publicity.
- To protect our organization's good-will.
- To avoid the time and cost of incident investigations.
- To avoid embarrassment for the organization and potential victims.

ADDITIONAL BACKGROUND

Imagine. Someone is secretly recording in your workplace. It could be an employee, a visitor, or anyone with espionage or voyeurism in mind. Their tool could be an app on a smartphone, a recorder disguised

as a USB stick[1], or a recorder that captures both audio and video hidden in a fake key fob, pen or wristwatch. In fact, recorders are being secreted into all sorts of everyday objects.

The bad news is you won't realize it has happened until it is too late. The first sign of covert recording is often a lawsuit, lost competitive advantages, or the embarrassment of voyeuristic footage being sold on the Internet.

Surreptitious recordings are usually prompted by one of four motivating factors…

INDUSTRIAL ESPIONAGE

This is the theft of trade secrets by the removal, copying or recording of confidential or valuable information.[2]

EMPLOYEE / MANAGEMENT RELATIONS

These are problems that management and the Human Resources department face. Here is a chilling statistic. One-third of employees who visit the U.S. Equal Employment Opportunity Commission (EEOC) office to file discrimination complaints bring with them secretly made recordings.[3] Katrina Patrick, a lawyer who represents aggrieved employees, says that more than 50 percent of the people who come to her office bring digital evidence. Some cases are settled for six figure sums.[4] One case is now in its eighth year.[5] Obviously, not anticipating surreptitious recording is expensive.

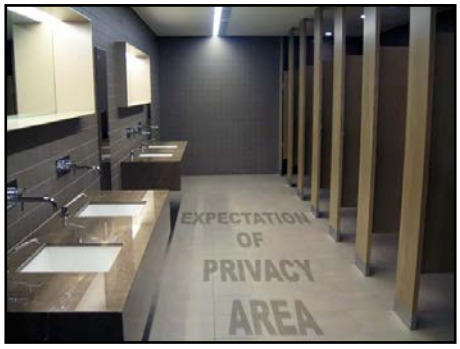
BLACKMAIL

Sometimes recordings are used to force outcomes. There is one news report of three employees who *bugged* their boss for a promotion, literally. They hid a recorder in his office and tried to blackmail him using the video footage.[6]

The last major motivation for illegal recording in the workplace is the focus of this training.

VOYEURISM

Almost all organizations are vulnerable to electronic voyeurism. Any place offering employees, customers, and visitors a space where personal privacy is expected is at risk.



We call these ***Expectation of Privacy*** areas, or **EoP** for short. Very few organizations are exempt from this threat. Remember, if you have a restroom, you have a risk.

---

[1] http://youtu.be/_9sPngNqsfA

[2] http://www.investopedia.com/terms/i/industrial-espionage.asp

[3] http://www.chron.com/business/sixel/article/One-third-of-workers-with-beefs-tape-their-bosses-1684505.php

[4] http://www.businessinsider.com/smartphones-spying-devices-2011-7

[5] http://spybusters.blogspot.com/2014/01/the-annabel-melongo-eavesdropping-case.html

[6] http://spybusters.blogspot.com/2013/10/bugging-boss-for-raise-lands-three.html

Thank you for downloading…

this preview version of the 25-page course text.

- About the Course
- Course Syllabus
- Introduction
- Law
- Strategy
- Identification
- Inspection
- See Through Black Plastic
- How to Handle a Find
- EoP Area Inspection Log

Please enroll in the **Spycam Detection** training course to receive the rest of this informative text.

http://counterespionage.digitalchalk.com