

What Should I Look for When Purchasing a Security System?

Patrick M. Murphy CPP, CLSD

June 21, 2004



Agenda

- Reasonable Care or Too Much Care
- Typical Design Mistakes
- Developing an Effective Design
- Potential Strategies, Solutions
- FYI Regarding Surveillance Systems
- Summary

Reasonable Care

Businesses are not the insurers of customer safety but have an obligation to provide a Reasonable Standard of Care

What is Reasonable?

- Crime must be foreseeable
 - prior instances of similar and total crime on premises
 - crime in surrounding community
- Personal injury, property loss, or damage must occur
- Failure to provide reasonable security must be the proximate or “cause in fact” of the crime committed

Too Much Care

- Expectation of privacy
- Reasonable expectation of immediate response
- Do you really want this recorded?

TYPICAL DESIGN PROBLEMS

- Focus on Threat Vs Risk
- No Vulnerability Solution
- No Requirements Defined

Objectives of an Effective Design

- What Is to Be Protected?
- Protected Against?
- Consequence of Loss?
- Level of Protection?
- Type of Protection?
- Protection Constraints?
- Integrated System/response?

BASIS OF AN EFFECTIVE DESIGN

- Risk Analysis*
- Functional Requirements
- Strategies/Solution
- Cost Analysis*

Risk Analysis

- Asset Appraisal
 - Identify and prioritize assets to be protected
- Threat Assessment
 - Define threat by evaluating the intent, motivation and tactics of the perpetrators
- Vulnerability Assessment
 - Identify how specific weaknesses may invite and permit the execution of the threat

Risk Analysis (cont.)

- Risk Assessment*
 - What are the consequences of loss event
 - Frequency, Probability and Criticality of event
- Three Options
 - Accept the risk
 - Mitigate the risk
 - Eliminate the risk

Risk Analysis

Suicide Bomber

- Asset Appraisal
 - Identify and prioritize assets to be protected
 - Crowds/gatherings of people in hotel
- Threat Assessment
 - Define level of threat by evaluating the intent, motivation and tactics of the perpetrators
 - Create fear, cause death-religious-bomb vests in crowded areas

Risk Analysis (cont.)

- Vulnerability Analysis
 - Identify how specific weaknesses may invite and permit the execution of the threat
 - Open, easy access to function areas
- Risk Assessment
 - What are the consequences of loss event
 - Multiple deaths, PR, loss revenue
 - Frequency, Probability and Criticality of event
 - 0 in USA - low - moderate to high

Risk Analysis (cont.)

- Three Options
 - Accept the risk
 - Mitigate the risk
 - Eliminate the risk
- **Accept**

Risk Analysis

Hotel Systems Computer Room

- Asset Appraisal
 - Identify and prioritize assets to be protected
 - PMS, NGS systems
- Threat Assessment
 - Define level of threat by evaluating the intent, motivation and tactics of the perpetrators
 - Disruption, loss of revenue-revenge (ex-worker) political (PETA)-insert virus, cause physical destruction to equipment

Risk Analysis (cont.)

- Vulnerability Analysis
 - Identify how specific weaknesses may invite and permit the execution of the threat
 - Door left unlocked, unaccounted keys,
- Risk Assessment
 - What are the consequences of loss event
 - Hardware \$80,000, loss of NGS business data \$millions, manual check-in process \$, guest complaints\$, recovery of data \$, poor PR, loss revenue
 - Frequency, Probability and Criticality of event
 - 0 - moderate - moderate to high

Risk Analysis (cont.)

- Three Options
 - Accept the risk
 - Mitigate the risk
 - Eliminate the risk
- Mitigate

BASIS OF AN EFFECTIVE DESIGN

- Risk Analysis*
- Functional Requirements
- Strategies/Solution
- Cost Analysis*

Security Program Functional Objectives

- Deter
- Deny
- Detect
- Delay
- Respond
- Communicate
- Assess
- Surveil
- Display
- Monitor
- Command
- Respond
- Intervene

Functional Requirements

- Is a Statement of Security Objectives (not required protective measures)
- Focused on assets and threats
- Addresses Vulnerabilities
- Includes levels of protection (optional)
- Provides guidance for designer

Functional Requirement

Example

- Vulnerability:
Access to computer room is not controlled
- Level of protection: moderate
- Functional Requirement (statement):
Limit access to computer room only to employees who work there with a *high probability* of identification

Functional Requirements

Example Statements

- Ensure response to crisis/disaster through detailed procedures
- Detect unauthorized entry into facilities from 11:00 pm to 6:00 am
- Control access into non-public areas of facilities.
- Provide for continuous surveillance of site entrances, lobbies and loading docks.

BASIS OF AN EFFECTIVE DESIGN

- Risk Analysis*
- Functional Requirements
- **Strategies/Solution**
- Cost Analysis*

Strategies

- To include but not limited to:
 - Policies & procedures
 - Personnel
 - Training
 - Electronic systems (alarm, CCTV, locks, etc)
 - Barriers (physical & psychological)

Strategy (recommended solution)

Computer Room

- Install a card reader lock with interrogation capabilities.
- Install a CCTV camera to identify persons entering & exiting the room.
- Create policy
- Train affected associates

BASIS OF AN EFFECTIVE DESIGN

- Risk Analysis*
- Functional Requirements
- Strategies/Solution
- Cost Analysis*

Cost Analysis*

- Cost Vs Benefit
- Determine actual cost of proposed program (include ongoing maintenance)
- Determine impact of loss, financially or otherwise
- Compare

Cost Analysis

Example

- Card reader lock \$200, CCTV camera \$800, policy \$30 (time), training \$60 (time), total **\$1,090**
- PMS, NGS & additional hardware \$80,000, loss of NGS business data \$millions, manual check-in process \$, poor GSS \$, recovery of data \$, mental anguish priceless, potential total **\$ millions**

Potential Strategies, Solutions

- Access Control
- Guestroom Safes
- Alarm Systems
- Communications Systems
- Record Keeping Systems
- Crime Prevention Through Environmental Design
- HVAC

Access Control

- Parking lot
- Public space
- Guestroom
- Back of the house

Access Control Parking Lot

Bollards & Barriers



Active Barriers



Overly Active Barriers



Parking lot controls

- Card readers on gates (arm or roll up)
- Card readers on tire shredders
- Security officer booth

Access Control Public Space

Electronic locks

- Lobby entrance
- Public entrances
- Guest elevators
- Pool & health club
- Business center, guest laundry, etc

Guestroom Electronic Locks

- PMS interface (accurate info, rm# chck/out)
- Ability to interrogate
- Auto deadbolt
- Smartcard/bio-metric
- Wireless
 - Swatch watch
 - Bluetooth
- Lock to CPU communication

Back of the House Lock System

- Same lock system as guestrooms
- Specific software for BOH
- Employee entrance (ID card)
- Control access to specific areas (FD, Acct.)
- Storage room, linen rooms, linen chute, etc.
- Smartcard master key interrogation
(Terminex contractor)
- Electronic combination locks that can be interrogated.

Guestroom Safes

- Enterprise interface (MATV, phone, AC)
- Checkout flag
- Daily vacant room report
- Eliminate or reduce rates for specific groups
- Ability to interrogate safe
- Ability to interrogate encoder
- AC outlet
- Biometrics

Alarm Systems

- CCTV integrated
 - preposition points (motion sensors)
 - record real time
 - full screen monitor
- Notification to pager/radio
- Delayed egress
- Holdup buttons

Communication Systems

- The Scan (PD to hotel security)
- MRTI 2000 (phone to radio)
- Nextel (buyer beware)
- Companion Phone (wireless front desk)
- Intercoms (garage)
- Radios for all public area associates
- House phones (emergency pool/gym)

Record Keeping Systems

- Electronic patrol documentation
- Incident reporting & tracking software
- Web based S.O.P.s & training
- Lost & Found tracking software
- Shipping & Receiving software

CPTED

- Lighting
- Minimize points of entry
- Minimize areas of hiding (persons/bombs)
- Create open line of sight

HVAC

- NBC detection system
- NBC filtration system
- Alarm/CCTV monitoring
- HVAC Emergency shut off plan

FYI CCTV Systems

CCTV Systems Pros

- Can be an effective tool for evidence
- Can be a deterrent
- Can be used for ID verification
- Effective means of identifying cause of alarms

CCTV Systems Cons

- Expensive
- Poor quality play back
- Create a False Sense of security
- Create a greater liability
- May record something you don't want

Camera Functional Description

- What is purpose of camera
 - deter criminal acts
 - produce evidence (record only)
 - catch the criminal in the act (record & monitor)
 - what type of activity is the camera monitoring
 - crowds forming
 - suspicious vehicles
 - suspicious activity (loitering, pick pocket, etc)
 - positive identification
 - public area
 - back of the house

Camera Functional Description

(cont.)

- The field of view must be specified for each functional description. This is measured by the percentage of screen a 5' 10" person will take up on the screen.

General monitoring 5%



Detection of Activity 10%



Recognition of known indiv. 50%



Recognition of unknown 120%



Camera Functional Description

Example

The function of the camera is to positively identify persons exiting the associate entrance and identify articles that they may be carrying i.e., purse, brief case, duffel bag, packages, etc. The camera is for the sole purpose of gathering evidence and need not be monitored. The camera need only to record while activity/motion is occurring within it's view.

Best Practices

- Public space cameras monitored 24/7 by trained personnel at security or telephone operators.
- No dummy cameras
- No audio recording or monitoring (WTA)
- Remote CCTV monitoring
 - Must have direct contact with response personnel

Best Practices (cont.)

- Pan/Tilt/Zoom, often 2 to 3 fixed cameras are more effective and cheaper
- Try to integrate alarm points with all cameras
- When monitoring, only monitor public area cameras through full screen switcher
- 640x240 pixels minimum resolution, 240 lines analog
- Resolution of camera and recorder should be of equal value
- VHS tape life, approx. 30 passes

Digital Surveillance Systems

- Convenient video storage
- Remote/internet access
- Easy playback
- Motion detection within camera
- Recording speed for different intents
 - Identification 2 fps
 - detailed hand movement 10 to 30 fps
 - happy medium approx.. 4 fps

Digital Surveillance Systems

- Frames per second of DVMR indicate all cameras at once (32 fps, 16 cameras= 2 fps per camera)
- Digital systems should only record when motion is within screen
- Use JPEG or Wavelet compression for PTZs
- Buyer beware in regards to storage compression (resolution or fps or number of days recorded)
digital cassette

Summary

- Complete a Risk Assessment – define your vulnerabilities
- Create functional requirements – define your end result
- Ensure the strategies/solutions meet the needs of the functional requirements
- Weigh the cost vs. the loss

Reference

General Security Risk Assessment Guideline

www.asisonline.org