Physical Security Audit Checklist

Performing regular security audits is a best practice that every business should follow. Every location is vulnerable to threats, be they physical theft, information theft, life safety risks to employees and patrons, and/or acts of God. A survey performed by the NRF revealed that in 2012, organized retail crime was the highest it has been in 7 years. Nine out of every ten retailers were affected by organized retail crime[1]. The annual Theft Survey performed by Jack L. Hayes International found that shoplifters and dishonest employees stole over $6 billion in 2011 from 24 major retailers[2].

The best planned security systems and security procedures lose their effectiveness if they are not continually monitored. Store managers should perform regular security audits on an interval determined by senior management. Management should also establish criteria for when additional unscheduled security audits should be performed, such as a change in location, a new threat, suspicion of loss or actual loss, etc. A mechanism to communicate the findings of the security audit back to management, as well as to ensure action is taken on any shortcomings also needs to be developed. Security audits can encompass a wide array of areas; however, a cursory checklist is below.

Security Audit Checklist

Physical layout of the organization's buildings and surrounding perimeters

- Does the property topography provide security or reduce the means of attack or access?
- Does the landscaping offer locations to hide or means of access to roof tops or other access points?
- How many points of entry are there to the building? Are those entrances monitored?
- Do all persons entering and exiting the building go through a security check point?

Lighting

- Is there sufficient lighting to allow guards, employees, or others to see places of possible concealment or access?
- Are access points obscured by low light?

Alarms – including fire, intrusion, tamper, motion

- Are doors, windows, gates, turnstiles monitored for egress and ingress?
- Are means of ingress able to be audited to identify who accessed those areas?
- Is the premises monitored for fire or smoke? Does the system alert the local fire department?
- In the event of a forced entry who does the alarms system notify? Is it monitored by a third party or staff?

Physical barriers – including fences, bollards, tire strips, gates

- Are fences tall enough to reduce unauthorized access to the property? Is the fence checked regularly by staff for holes, damage or access points.
- Are bollards in place to prevent damage to buildings or access points by vehicles?
- Are tire strips installed and able to be used to prevent unauthorized entry to sensitive areas around the property? Parking lots, loading docks, pick up areas.

- Are gates secure and operating properly?
- Is entry to the premises protected by gates or is vehicular traffic allowed to move freely on and off the property?

Access points – including doors, gates, turnstiles, windows, docks, elevators and stairwells

- Are doors and gates in good working order? Do they operate properly and close on their own?
- Do turnstiles operate properly and are credentials required to go through?
- Are windows locked if they are able to be opened?
- If large panes of glass are installed in the building, are they laminated with a security film to prevent forced entry?
- Do docks and dock doors operate properly, and are they locked when not in use?
- Are elevators and stairwells checked for daily or hourly by security staff?

Guards

- Does the organization's property utilize a guard staff?
- Do guards verify persons coming on the property are allowed access? How do they verify? ID, Verify with staff members, inspect vehicles, record names and license information?
- Do the guards make rounds on the property to check places of access? Doors, windows, elevators, stairwells, dock or bay doors, secured areas?
- Do guards complete check sheets while on duty to verify they checked as directed?
- Do guards vary their patrol patterns to reduce the chance of their routines being exploited?

CCTV

- Are the perimeter of the building and the perimeter of the property adequately covered by cameras?
- Are cameras able to switch automatically from daytime to night/low light?
- Are the building entrances and exits monitored by cameras?
- Are stairwells and other access points monitored by cameras?
- Are the cameras monitored 24 hours a day or only reviewed after an incident has taken place?

Access methods – including locks, proximity cards/swipe cards, code or cipher locks, and other credentialing methods.

- Are locks and locking equipment in good repair and operating properly?
- Do past employees still have keys/access cards to the building?
- Have past employees/ terminated employees been removed from having access to the property?
- How often are codes changed on code or cipher locks?

Methods of communicating breaches found during the security audit to the persons responsible for the organization's security. Including – local alarms/lighting, phone, text, email etc…

- How are security personnel notified of breaches in security and unauthorized access? Guards, local alarms, monitored alarms, phone calls?
- Does your security staff know the organization's policies for notifying management or other key personnel?

Performing a security audit on a regular basis will help your organization minimize loss and increase the safety of employees and customers. With each audit, the facility will become increasingly less vulnerable.

The annual Theft Survey referenced above also found that the average case value to prosecute shoplifters and dishonest employees cost $150 dollars and 62 hours. Anything that can be done to reduce the chance of this happening to your locations will affect your bottom line and your organization's efficiency. A security audit takes minimal time to complete and will have lasting effects on increasing the safety and security of your locations.

---

[1] Grannis, K. NRF Report Finds No Retailer Immune to Organized Retail Crime. *National Retail Federation*. Retrieved January 14, 2013 from http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=1380

[2] Annual Retail Theft Survey. *Jack L. Hayes International, Inc*. Retrieved January 14, 2013 from http://hayesinternational.com/news/annual-retail-theft-survey/

Google

- About the Author
- Latest Posts

About Katie Willie

Katie Willie is the Marketing Director at LockNet. After growing up around LockNet, Katie formally joined the team in 2007. She manages the LockNet brand by developing and strengthening the marketing program. Establishing LockNet as a go-to-resource, she manages LockNet's content creation efforts. Outside of work, Katie enjoys chasing her toddler and playing with her dogs Cody and Ollie (LockNet's original Chief Morale Officers).

- Shoplifting Prevention: Four Products to Consider - February 4, 2016
- Theft Prevention: What's a Lock Got to Do with It? - February 3, 2016
- Pharmacy Security: The Essentials - January 28, 2016
- LockNet Employee Spotlight: Jeffrey Carroll - November 5, 2015
- National Locksmith Dispatching: Three Things to Consider - November 3, 2015
- LockNet Employs an Author: Whitney Fay - October 22, 2015
- Door Codes: Locks & Links - October 15, 2015
- History of Locks: A Crash Course - October 14, 2015
- Commercial Safe Answers: What You Should Know - October 6, 2015
- Secure Your Doors with Five Simple Products - September 30, 2015