Security101

The importance of concentric circles of protection

in municipal structures

Building a *comprehensive* program around *concentric circles* starts with the idea of viewing the building in layers that require distinct levels and measures of *protection.*

Security101

Contents

Introduction

As various ways of minimizing an excessive level of violence against the public sector are studied, it is important to visit the concept of *concentric circles* and how a layered approach to security can render outstanding results for governmental agencies, such as courts and police departments, who are repeatedly the victims of domestic offenders, disgruntled citizens, vindictive employees, and the mentally unstable.

Lack of respect for authority and absence of preparedness are two key factors that have increased the number of attacks against these institutions and their public functionaries. The widespread occurrence of this type of assaults obliges leaders and managers to develop thorough risk assessments and security plans. If a violent event is predictable — and it likely is — then, it is preventable.

Building a comprehensive program around *concentric circles* starts with the idea of viewing the building in layers that require distinct levels and measures of protection. Vulnerability evaluations, CPTED (*Crime Prevention through Environmental Design*), and expert knowledge on the most appropriate and advanced technologies are crucial enhancements when adopting a security in-depth vision.

The purpose of this approach is to effectively *deter, detect, delay, and respond* to crime. In public offices, the application of concentric circles, together with the implementation of the most suitable security products, can allow decision-makers to be prepared for even the most challenging scenarios, reduce possible fatalities and property damage, and ensure continuity of operations to remain being of service in their communities.

Understanding the threat

It is not uncommon to hear random shooters walk into a police station or a courthouse and injure public servants, like it occurred in New York in 2020, where a gunman was arrested after he ambushed police officers twice in 12 hours. Unfortunately, this is not a rare episode; violence against public institutions has evolved and augmented over time. Further, considering respect for authority has steadily decreased, municipal structures now lack the one element that used to prove effective when confronting emerging acts of violence.

Understanding who can be a threat to the institution is primordial to conduct a risk assessment and determine vulnerabilities, opportunities, and solutions. The threats include domestic violent extremists, protesters, rioters, and looters, disgruntled citizens, vindictive personnel, and people with mental disorders, in addition to gang members and convicted felons. Foreseeable tactics are edged weapons, small arms, and improvised explosive devices.

POSSIBLE CRIMINAL PROFILING

A person who might pose a threat to the institution may display one or more of the following characteristics:

- **Upset** – they had to take time off work without pay or maybe they have to pay a fine which they cannot afford.
- **Confused** – first time offender, slow moving lines, failure to understand instructions.
- **Concerned** – with the fine amount, the insurance cost, or possible jail time.
- **Angry** – feels unheard or misunderstood.
- **Expectant and impatient** – waiting for justice, resolution of conflicts, successful achievement of procedures.

HANDLING DIFFICULT PEOPLE

A serious situation may happen unexpectedly and demand immediate action. Normally, in any stressful scenario, a well-trained employee, experienced at dealing with a given incident, is much more successful compared with staff who does not know what to do or how to react. Handling difficult people is an art and requires skills and multiple forms of effective communication. Knowing how, when, and what to communicate is important to deescalate a possibly dangerous situation and calm down an angered citizen.

The following are some strategies that could alleviate the tension and avoid an assault:

- Remain calm
- Remove the audience
- Check your personal emotions
- Be mindful of body language
- Provide silence spaces within the conversation
- Use effective questioning
- Watch your tone
- Be empathetic
- Give choices

Security in-depth is common sense

The common piece of advice "*don't put all your eggs in one basket*" is entirely applicable when approaching security in-depth and applying concentric circles of protection to governmental offices. When leaders have multiple layers of protection, they do not rely any more on a single layer, which could be dangerously vulnerable and eventually breached by an intruder. Security in-depth is a commonsense method that naturally increases redundancy and lessens chances of criminal activity occurring in the premises.

Redundancy is fundamental. In case an intruder is successful at gaining access at one of the layers, he could be detected and stopped when attempting to enter another layer. An absolute minimum of three layers — ideally four or five layers— should exist between the outside world and any type of important assets (cash, arms, documents) within the building.

Security in-depth works best when strategically combined with CPTED (*Crime Prevention Through Environmental Design*). CPTED employs the 1 deliberate design of buildings, landscaping, and outdoor environments to discourage crime, minimizecriminal opportunity, and promote positive interactions. The three elements of CPTED are territoriality, surveillance, and access control.

FOUR STEPS FOR BETTER SECURITY: DETER, DETECT, DELAY, AND RESPOND

Physical security measures aim to protect people, information, and assets from compromise or harm with the following valuable techniques:

Deter

Deterring and discouraging crime is the first step. Implementing measures and obvious challenges to enter the site without authorization are vital, as criminals will perceive the government building as tough or needing special tools and training to gain access. It is ideal to dissuade assaults with physical deterrents, such as gates or fences, as well as psychological measures, like sufficient lighting and video surveillance.

Detect

How able is the system of the public building to detect an invader in action? and *What is the probability of detection?* Answering these two questions can provide a better understanding of the capacify of detection in the site. Moreover, it is of the utmost importance to assess the time it takes between alarm activation, by sensor devices, and the verification of the alarm. The longer the time, the more opportunity is given to the criminal to accomplish his goals.

Delay

Delaying relies on presenting the adversary with ample obstacles to increase the time he takes to perform a criminal activity. Fencing, bollards, access control points, turnstiles, and hardened rooms can cause delay and will require the invader to have a series of skills and tools in order to breach all layers of security. Delaying the criminal effectively will grant time to the organization to call for help and respond before it is too late.

Respond

An effective response faces adequately the criminal within an appropriate time frame. It also involves the communication capabilities between the public institution and first responders, as well as the accuracy of the information transmitted. Time of deployment of help by police and other authorities is vital to improve to efficaciously stop and apprehend the intruder.

BROKEN WINDOW THEORY

Concentric circles of protection and CPTED align with the interesting theory of the *broken window*, which states that visible signs of crime, anti-social behavior, and civil disorder tend to foster climates that encourage further crime and disorder. When buildings are designed taking into account territoriality, surveillance, and access control criteria and layers of protection are solidly defined and hardened, criminals take notice, leading to violence being effectively prevented.

Social psychologists and police officers agree that if a window in a building is broken, and is left unrepaired, all the rest of the windows will soon be broken too. Paying attention to problems when they are small and preparing for possible violent scenarios means problems are less likely to escalate and offenders are more reluctant to engage in criminal activity.

BASIC PRINCIPLES AND THE IMPORTANCE OF SYNERGY

1. Include multiple layers of security to decrease the likelihood of an aggressor gaining access to the public property.
2. Rates of success can be achieved by adding layers, or by increasing the robustness of each layer, or by doing both.
3. Never rely on a single layer of security. It requires an unattainable level of perfection and leaves no room for human error or equipment failure.
4. Procedures and technological solutions can enhance levels of security.

Security in depth is beneficial only when there is synergy between all components, measures, and layers implemented. Strategic coordination and synergism can prevent sloppy, inconsistent, or complacent actions. The strong connection of solutions adopted is necessary to protect employees, citizens, key assets, property, and very importantly, the public office's reputation.

Layers of security

Just as an onion is composed of multiple rings, security for a government building can be planned in various layers. Intendedly determining where employees and key assets are located and what assets are placed on the skin or outer perimeter of the site should be a priority. Further, installing the right solutions in each layer allows intruders attempting to penetrate the building to be timely detected and intercepted with a proactive and effective security response.

The concentric circles of protection get stronger with every integration of security hardware, starting from the outer perimeter and moving inward to internal areas requiring the greatest protection. Each of these circles demand human and physical elements, paired together in synchronicity to achieve the goals of hardening the facility, discouraging penetration, providing time for an adequate response, and keeping criminals out. Layers of security and enough countermeasures housed within the circles of protection can significantly diminish the likelihood of crime.

THE OUTER PERIMETER

This is the first line of defense. Having a clear boundary around the government site defines public from private property. A perimeter can be complex to define, however, it should include the outer reaches, meaning that parking lots and outlying buildings must also be considered. Establishing a robust outer perimeter ring can help prevent a surprise attack.

Natural or manmade barriers at the property line can be used to reduce vulnerabilities and gain time, like walls and fencing. Nevertheless, a successful strategy should include more than a clear boundary. Acknowledging the importance of outdoor lighting, landscaping, and signage (*e.g., Private Property: No trespassing*) is required, as these pose a psychological barrier for the offender and can dissuade him from committing the crime. Further, *advanced license plate recognition* (ALPR), *security fences*, and *gate control* are solutions that could be deployed in this concentric circle.

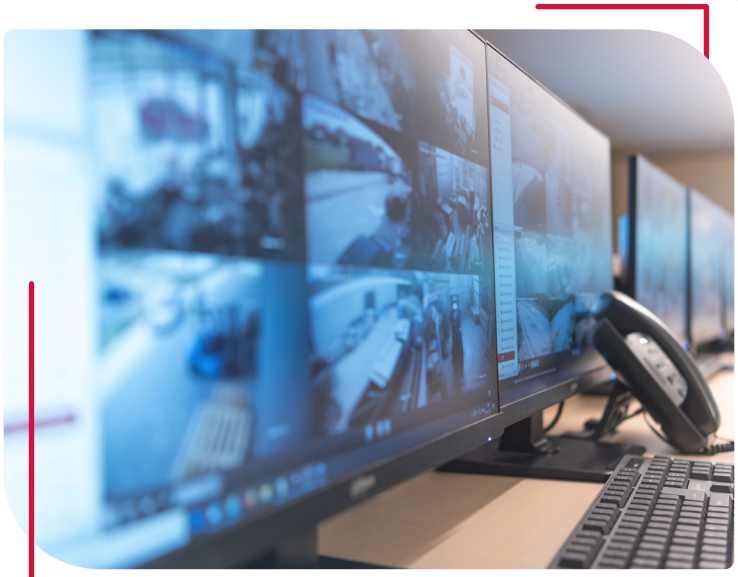
MIDDLE LAYER

This ring includes the open space that exists between the perimeter and the exterior of the building as well as the transition space, e.g., doors and windows. Deploying security cameras with advanced features is imperative for this layer of security, especially as they enhance vision from the building to the perimeter. Smart IP cameras, PTZ (Pan, Tilt, Zoom) cameras, motion, and IR infrared sensors can help the security team detect if there is a threat. Video analytics are equally important to access relevant data, detect vulnerabilities, and fix what is not working.

This layer is vital. If an intruder is able to cross the perimeter and the open space, he increases his chances of entering the building. Installing wireless locks, a first-class visitor system, and access control solutions in this ring are alternatives public institutions have to efficiently harden their facilities and prevent an emergency.

Practices and protocols are necessary too. Ensuring doors and windows are always closed/locked and not propped open, and getting rid of heavy objects like rocks near the building that could eventually be used to break in are examples of adequate behaviors and additional security actions.

INTERNAL AREAS



A modern video surveillance system, monitored by trained security staff; in conjunction with motion sensors, access control, and smart locks in interior doors can harden this fundamental layer of security, where employees and most important assets are located. As municipal buildings are open to the public throughout most of the day and they are a likely target for violent threats, ensuring this concentric circle is properly defined and secured with the latest technologies is imperative.

Access control that only allows authorized employees and a powerful visitor system can mitigate risks and increase confidence and a sense of security in personnel and citizens who must visit these public premises. Security awareness and training of employees on how to recognize an emergency and properly respond to it is also beneficial and highly recommended.

There are also invaluable assets that must be duly protected. These items should be housed in the inner ring of the site and additional measures should be taken to protect their integrity. For instance, if it is cash, it should be placed in a concealed and locked safe. In the case of computers, they should be backed up daily and be strongly protected with encryption or passwords.

Further, an emergency communication system is required at the core of concentric circles. Allowing leaders to send critical messages to their employees and visitors, in the case of an emergency, having the capability of a two-way interaction, and being able to communicate over different interfaces, can prevent injuries, the loss of life, and the damage of property.

Conclusion

Installing a structured security system in a government building requires more than a random deployment of products unable to work synergistically to protect what matters most—life, valuable material assets, agency's reputation, and property. A comprehensive risk assessment and a systematic and coherent methodology should be brought into play to identify security needs and guarantee they are properly addressed with state-of-the-art technologies and useful practices and protocols.

The concentric circles approach and the implementation of security in layers facilitates the hardening process and promotes the adoption of solutions that truly work well together, harden efficaciously the site, and prevent crime. Along with CPTED (*Crime Prevention Through Environmental Design*), security in depth is a valuable concept that should be utilized by the public sector, especially when a growing body of research supports the assertion that crime prevention through these methodologies is effective in reducing lawbreaking and fear in the community.

Understanding the basic application principles of concentric circles and making use of the required metrics of *deterring, detecting, delaying, and responding* are conducive to better performance and a more effective physical security plan. Depending on only one layer of security, as it is regularly the case, generates tremendous vulnerabilities for governing institutions. Conversely, security in layers provides a greater opportunity for public bodies to be successful in preventing crime.

Making access to intruders difficult with properly hardened rings will not only help discourage criminals from attacking the site, but even if they attempt to do it, they will take a longer time trying to defeat all obstacles on their way, providing the security team with a key factor: time. The possibility, therefore, of protecting people and assets and mitigating the consequences of an attack are high with the notable practice of concentric circles of security.

FIND A LOCAL OFFICE

Contact your local office today for an on-site, no-cost security assessment.
For more information call **800.261.2041** or visit **security101.com**