SECURITY EXECUTIVE COUNCIL

A research and advisory firm

Convergence and Layers of Security

Ray Bernard, PSP, CHS-III

Originally Published in SecurityInfoWatch.com

January 2010

Convergence and Layers of Security

Not only at the ASIS conference in September, but also at a few security events and meetings afterwards, I have been asked this question a number of times:

Q: Does security technology convergence mean that I need to be thinking differently about how I use technology?

Although the quick answer is Yes, thinking differently doesn't mean throwing away the perspectives about protective measures that have been effective in the past. Although security technology has changed significantly over the past decade, many traditional security perspectives have not changed. One such perspective is Layered Security.

Over the years, many readers have read at least some of the numerous articles and book chapters written on the topic of Layered Security. The reason this column presents the concept again is that today's technology gains provide opportunities to significantly improve the security layers of our facilities, and so nearly all security technology plans deserve a good review from this perspective.

Given today's economy, many trade journal and security conference discussions revolve around upgrading or enhancing technology rather than replacing it. Most of these discussions are based on technology perspectives. Unless technology perspectives are coupled with a security applications perspective, there is low assurance of receiving the security benefit that could and should result from security technology planning. Layered Security is one of the valuable application perspectives.

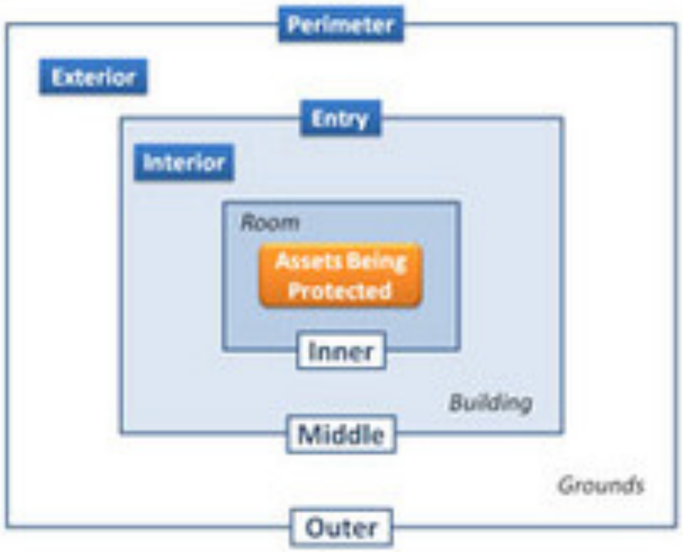
Security Layers

Layered Security is a design concept. It has also been called "concentric circles of protection" and "compartmentalization." This concept is part of the concepts included in Crime Prevention Through Environmental Design (CPTED). The first illustration in Facilities Physical Security Measures, the recently released ASIS guideline (free to members through the ASIS online bookstore), presents a simple layered security concept of three layers:

- Outer Protective Layer – e.g., natural or man-made barriers at property line
- Middle Protective Layer – e.g., exterior of building
- Inner Protective Layer – e.g., doors within building

As the standard states starting on page 7, “One of the basic CPTED strategies is to design multiple or concentric layers of security measures so that highly protected assets are behind multiple barriers. These layers of security strategies or elements start from the outer perimeter and move inward to the area of the building with the greatest need for protection. Each layer is designed to delay an attacker as much as possible. This strategy is also known as protection-in-depth (Fay, 1993, p. 672). If properly planned, the delay should either discourage a penetration or assist in controlling it by providing time for an adequate response.”

It is important to understand that the standard’s layers of security illustration is an example of applying the design concept, and that you as a practitioner should apply the concept as appropriate for the facilities you are protecting. The example is intentionally simple, whereas facilities are often more complex, having multiple buildings and multiple asset locations within each building. The graphic below expands on the picture presented in the ASIS standard, naming four layers of security (Perimeter, Exterior, Entry and Interior) to facilitate thinking about how technology can be applied.



Layers of Security Concepts

This chart expands on the picture presented in the ASIS standard, naming four layers of security (Perimeter, Exterior, Entry and Interior) to facilitate thinking about how technology can be applied.

Security Functions by Layer

With respect to harmful actions against an asset, protective measures are intended to provide one or more of these basic functions:

- prevent (hazard condition or attempt by threat);
- deter (access or attack by an active threat);
- detect (presence of hazard or threat);
- delay (access or attack action);
- assess (situation);
- respond (by denying access, inhibiting attack actions, defending or protecting assets, minimizing consequences); and
- recover (from effects of the attack).

One good way to approach technology design is to ask two questions for each security layer you have identified: What security functions should we implement? and What technology will support those functions?

If you have convergence experience you want to share, e-mail your comments to me at **ConvergenceQA@go-rbcs.com** or call me at 949-831-6788. If you have a question you would like answered, I'd like to see it. We don't need to reveal your name or company name in the column. I look forward to hearing from you!

*Ray Bernard, PSP, CHS-III is the principal consultant for Ray Bernard Consulting Services (RBCS), a firm that provides security consulting services for public and private facilities. Mr. Bernard has also provided pivotal strategic and technical advice in the security and building automation industries for more than 22 years. He is founder and publisher of The Security Minute 60-second newsletter (**www.TheSecurityMinute.com**). For more information about Ray Bernard and RBCS go to **www.go-rbcs.com** or call 949-831-6788. Mr. Bernard is also a member of the Subject Matter Expert Faculty of the Security Executive Council (**www.SecurityExecutiveCouncil.com**).*

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year "retained" services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com