Minieri's

# "GLOBAL TOP 10 Security Department Deficiencies"

2020

MINIERI
ASSOCIATES
INTERNATIONAL

*Worldwide Consultants & Engineers in Physical Security, Fire Protection & Life Safety*

# Minieri's
# *"GLOBAL TOP 10 SECURITY DEPARTMENT DEFICIENCIES"*
# *2020*

After 45 years of protecting lives & property for well over 1000 facilities, in more than 35 countries, I've found a noticeably common recurrence of certain security department deficiencies. Here are my **TOP 10** emphasizing consideration of *CRITICALITY in overall effectiveness in the Department's mission* and the probability of long-term *MANAGEABILITY for success in maintaining the Department's objective*. I'll keep this brief.

## #10 – CURRENCY

Experienced security professionals know that security technology has a limited life cycle. Five years should be expected and any years beyond that are a bonus. Like all technology, it tends to evolve and get more effective and useful on a frequent basis these days. Over time, replacement parts may no longer be available. A major effort must be expended by security consultants and engineers – AND security management - to keep up with the most current technologies. It is possible in many cases to upgrade entire sub-systems – like perimeter detection or systems management integration – without doing it all at once. Proven strategies can let you budget the investment over several years in an "evolutionary" manner, vs. a "revolutionary" step. Metrics will allow you to track the costs of repairs to find that point where it becomes more "cost-effective" to begin the replacement process. Test everything regularly, frequently and thoroughly … and get it back online ASAP!

## #9 – DISTRACTIONS

Tasking Security Personnel to non-security duties is a "no-no" and most people know this. So why do others in the organization – heads of other departments in particular – think those people are available for additional responsibilities? They just observe them "*standing or walking around*" and assume they have nothing useful to do. I have seen many amazing examples including hotel lobby guards doubling as the "doorman" or even doing "valet parking" or delivering the mail. I once knew a guard contractor named "*Janitor with a Gun*" which is self-explanatory. You have had no recent losses so it may appear to others that the COST of security should be offset through such practices. Don't do it. If you can task a guard like this without critical security risks, you probably don't actually NEED that position at all.

## #8 – MAINTENANCE

I like to compare the preventive maintenance and repair programs in an organization's "Security Technology" vs. its "HVAC" system. Surprise, surprise … HVAC often wins out. If upline executive management does not recognize the risks of allowing security vulnerabilities and failures - just wait - after the horse gets out of the barn, they will allocate the funds to fix the latch on the barn door. You can say "*I told you so*" on the way to your car after termination or to your deposition if you're lucky. Metrics on your technology downtime are a fundamental tool for undertaking this battle. Build your case and present it with confidence by showing your degrading trend and increasing costs.

## #7 – PROCUREMENT

The constant excuse for poor results from technology and services procured is "LOW BID". I hear this in most government engagements and often in large corporate enterprise environments. The implication is that the lowest bidder will always be inferior and this is not necessarily true. The root of poor results in procurement of security goods and services is most often a result of POOR SPECIFICATIONS in the tender, RFP or RFQ. This implies of course, that the one writing the specifications is knowledgeable of the tiny technical details and the available state-of-the-art features so that the bids clearly limit qualification to "*what you need and want*" and so that submittals are "*apples-to-apples*".

## #6 – ASSUMPTIONS

This refers to cases where those responsible for Security have – unintentionally and unthinkingly - come to a certain comfort level regarding the protection afforded by the measures they have in place. If one does not hear of any failures, breaches or attempted attacks, it is easy to assume it is due to their "good security". More often than not, this situation results from a "*lack of attempts*". Be diligent in looking for your vulnerabilities … *that's what your adversaries are doing.*

## #5 – COMPLACENCY

It is still too common to discover a guard sleeping on duty, most often on the night shift of course. But it is not just the guards who are sometimes guilty of complacency. Those in supervisory and managements positions tend to visit all guard post less and less frequently over time, particularly when things seem to be running smoothly. Time spent constantly "searching" for non-compliance with security documentation is time well spent. There are many creative methods of "*keeping everyone on their toes*".

## #4 – TRAINING

When it comes to the Guard Force – particularly if outsourced – training is almost certainly the most common complaint and has been since I started in this profession in 1974. In general, it is probably better today than ever before, but extremely FEW Security Departments will have the necessary finances to INVEST in a comprehensive, well prepared and delivered training program. Additionally, training is NOT a "*one-time thing*", it's ongoing and must be a part of every annual budget.

## #3 – METRICS

"*We can affect only what we measure*" I've always said. Does your Security Department need to "improve"? Improve WHAT? Are you doing better or worse than LAST YEAR? …and so on. This should be considered a sub-element within the issue of *Documentation.* There must be a good system in place for recording, tracking and comparing a variety of key aspects of your Security Department performance.

## #2 – DOCUMENTATION

This was a tough choice as a contender for the #1 spot. One of the rarest elements I find with any Security Organization is a complete and comprehensive set of written documents. On those few occasions when I find ANY documentation, it is almost never written using terminology that is "*measurable and/or observable*". It is among the most difficult undertakings to write security policies, procedures, standards and guidelines that can be "*objectively*" audited for compliance. It's been said that "*a person cannot reasonably be held RESPONSIBLE for something they do not know and understand and a person that knows and understands CAN'T HELP but be held responsible*."

## #1 - HOLISTICS

There are 3 critical elements of physical security: Operational, Technological and Architectural Security and all 3 are inter-connected. In many different forms, I often see a *"perception of security"* rather than actual "*effective*" security in reality. A common example is an over reliance on technology without the absolutely necessary supporting components from the Operational and Architectural elements.

**A White Paper By:** Michael Minieri CPP, CSC, CPOI, CSM, CET, CST, CFPS, CCO

**About the Author:** See Michael Minieri's full C/V online here or visit www.MinieriAssociates.com