by Michael E. Marotta
Senior Technical Writer
Intentional Privacy, Austin, Texas.
www.intentionalprivacy.com
Michael.Marotta@IntentionalPrivacy.com
also
NecessaryFacts.blogspot.com
Uszik11@gmail.com
Physical mail:
6800 West Gate Boulevard #132-227
Austin, Texas 78745-4868
Mobile: 734-223-9054

➤ You need to view the slide deck. These are my notes for speaking while the slide is displayed. I do not (usually) just read the slide. These are two independent but co-joined narratives.

Slide 1: OWASP required title slide

Slide 2: About Me

I got into technical writing on a database project for General Motors in 1984. No one wanted to write the user manual and having published half a dozen articles and written two small books, I did the documentation. One thing led to another, and I became a full-time technical writer. But programming was always there. For instance, TeX/LaTeX was a mark-up language which led to SGML which led to HTML.

After the Dot.Com Meltdown and 9/11, work got hard to find, and in addition to being a sales clerk at the Atomic Energy Museum in Albuquerque, I got a job as a security guard. So, when my wife, Laurel, and I decided to go back and actually finish the four-year degrees we never needed when all you had to do was work hard and be smart, I got my degree in criminology. My social science degree is in transnational white collar crime/

Slide 3: Me in Uniforms
Upper left: I worked rock concerts in a red t-shirt and did well at it. So, they put me in the uniformed division and made me a dispatcher. I worked in campus safety as a patroller at Washtenaw Community College in Ypsilanti, Michigan, and I have a story about that later. Most recently, here and now, I am a member of the Texas Military Department, Texas State Guard, Maritime Regiment. In this picture, I was evaluating a dive team that extracted a vehicle from a lake. Mostly, I teach computer operations with WebEOC, the virtual emergency operations center. Right now, for the past four months, I have been assigned full time 24/7 to the Joint Force Plans Group of Domestic Operations.

**Slide 4: ISO/IEC 27K**

ISO is the international standards organization. Less well known is IEC the International electrotechnical commission. The IEC is 110 years old and is the result of work done by British and American electrical engineers at the previous turn of the century.

ISO 27K is a suite of standards, about 20 of them.

“The nice thing about standards is that there are so many to choose from.”

ISO 27K is just a standard, like Carnegie Mellon’s Capability Maturity Model, or what we called Value Engineering in the 1970s. What they all have in common is that you must demonstrate a method for improving the method. It is not enough to just do it right once. You must continually improve.

**Slide 5: ISO 27002 Only Applies to Software**

So, what we are going to investigate today is beyond 27002, but, really is fundamental to it.

**Slide 6: Developing Your Own Guidelines**

And ISO 27K allows this. In fact, ISO 27K requires this. You have to go beyond the minimums. You have to demonstrate that you not only meet the published standards but exceed them. In the military we say that if you are early you are on time and if you are on time you are late and being late is not acceptable. Same here. It is integral to the ISO 27000 suite of
standards that your implementation of them be validated as being extensible from them. In other words, you have to show not just improvement, but improvability.

**Slide 6: Developing Your Own Guidelines**

This gets complicated. You have to have standards for everything you do, which is about 100 or 1000 separate items. It is the kind of thing that keeps managers awake at night. But let’s just look at one discrete item: Visitors.

Is that person expected? Do you have a log that shows expected contractors, visitors, corporate liaisons, marketing partners, or whatever? Unless you are like Wal-Mart, walk-ins should always be considered dangerous.

OK. So, I was working as a security guard at the Littlefield Building at 6th and Congress and just before 0600 this contractor comes in. I look in the log and I cannot find his name. So, I give him the log to view and he cannot find his name. So, I denied him access. He went home, called his boss, who called up the chain and the next day, I got a reprimand. They called it a verbal counseling but it came with written documentation that I had to sign, so it was really a written reprimand. The contractor was really a subcontractor, just a guy working for a guy. He did not recognize the name of the general contractor, which was indeed in the log book. So, I got the reprimand. But ask yourself this – suppose I got fired. Do you want to tell your next interview that you got fired for not granting access to someone who was authorized for it, or that you were fired for granting access to someone who was **not** authorized for it? I was willing to take the hit. In fact, I was not fired.

**Slide 7: Physical intrusions are three times more prevalent than malware.**

These numbers come from the Verizon Data Breach Investigation Report of 2016. We get the Verizon security person to come speak at I-S-S-A. You should attend if you can. The report is available online. Look for Verizon D B I R

So, you can have all the firewalls and encryption and SHA128 you want, but if I can walk in and put a USB drive on a computer, I pone you.
**Slide 8: Zero Point 27 Percent.**

You spend about one quarter of one percent on physical security. Not only are you vulnerable. I am willing to bet that you have been compromised. Moreover and more to the point, you have not even detected the breach.

**Slide 11:**
This is the Iraqi information minister announcing that the Americans had been stopped outside Baghdad. Meanwhile his troops were shucking their uniforms and running away. The Americans were just taking a break, having driven right through the Iraqi defenses at 50 miles per hour for 36 hours. They were stopped because they were sleeping.

For your data center this means that you cannot just intend to stop penetration. You have to have an active offensive response to intrusion.

Ever mindful of the dangers of false arrest and false imprisonment, do you have a secure location in which to trap and hold an intruder?

Do you have anything that resembles a physical honey pot? How about a thumb drive left on a computer at a workstation? Hard to resist... What if removing the thumb drive broke a light beam that relayed all of the doors in that area to lock?

**Slide 12: Personal Information Stolen.**

This is not theoretical or hypothetical or suppositional. It is real. Data centers have been breached just for their hardware. When I worked as a security guard downtown, it was apparent that there are thieves who work the high-rise office buildings. They walk the floors looking for laptops to steal.

In the story at the top, the loss was of USB drives from the car of an office worker. So, you need auditable controls to prevent people from taking work home from the office.

The one on the bottom is from SlashDot. This data center was hit four times in two years with physical intrusions. I found other similar stories about Vodaphone in the UK. This one bears looking into because the
stories – this one in SlashDot and others from other sites – have discrepancies in their accounts. It seems that the so-called night security manager – probably the only guy on duty, which is an attempt to cheap out on security, having just one guard on duty – ignored the sounds of the thieves cutting their way in through a wall. But, there’s building maintenance all the time and the facilities management does not always inform security about what is going on. And it might have been the building next door. So, you need to form communities. Strong communities prevent crime. There is a crime triangle: It takes a willing perpetrator, an available victim, and the lack of a capable guardian. That capable guardian could be just a neighbor on a porch watching the street.

I just want to note that in this case, the guard was tazed and pistol whipped. I suppose that from your point of view, if it was just the guard, you don’t care, but what if it was you working late who got beaten and shocked.

**Slide 13: Escaped Inmate Captured.**

He was captured inside a data center. He walked away from a work detail. He found a broken door and slipped in. The security guard detected the intruder – probably on camera – and almost called the police once… when the police dispatcher got the 9-1-1 hang-up call from the data center, the cops were sent over. The guard led them through part of the building and they did not find anything, so they left. That was about 2:30 AM. The guard then spent the time required to review all of the camera logs and at 3:46 AM called the police again. They swept the building and flushed the convict. The guard then found the broken door by which the escaped prisoner had gained entrance.

**Slide 14: How to Break in to a Google Data Center.**

It is not a question of “if” but of “when.” What are you going to when your controls fail and the intruder is inside the perimeter?

**Slide 14: Domestic Workplace Violence**

According to ISO 27002, you protect your human resources by protecting their personally identifiable information. ISO 27K says nothing about their physical safety.
As a security guard, I have had the phony boy friend show up with flowers. Failing at the front desk, he tried the back dock, but the woman on guard there was not someone you want to confront, so the phony boy friend left. My boss counseled the intended victim on the incident.

**Slide 16: Low Esteem**

That boss of mine was a retired Detroit police officer. It is pretty common. In fact, it prevented me from getting into management because I was never a cop and not likely to be. Just know that when you diss your guards, you are denigrating the people who are between you and harm.

**Slide 17: Marvin**

Here I am, brain the size of a planet, and what do they have me do? I am going to continue to make the case that you are under-utilizing your security guards.

**Slide 18:**

Let’s get some perspective here.

**Slide 19:**

Another woman lost to history. Joan Clarke had another life after Turing and Bletchley Park. I wrote a biography of her being awarded a gold medal by the British Numismatic Society for her deciphering of the gold coins of Scotland.

**Slide 20 Law and Order (No comment.)**

**Slide 21: Yellow Rose**

But it was not always so... American fought a two-front war involving rockets and atomic bombs and Roy Rogers played an insurance investigator, not a sheriff or marshal...

**Slide 21: Black and White Television**

Before the frontier territories were federalized, Wells Fargo had its own detective agency. Before Miami Vice the private detectives of Surfside Six tracked criminals in Miami. Before Hawaii 5-Oh, which made “Five Oh” gang talk for police, there were the private services of Hawaiian Eye. Paladin was the code word for a gunfighter who stood up for the
defenseless. Have Gun: Will Travel. Wire Paladin, San Francisco. If you understand when old technologies were new, everyone else had a name. He had a username on an information system.

Private security was not always Paul Blart Mall Cop.

**Slide 23: Twin Towers**

You never hear about them. We honor the fire fighters and the police, rightfully so, but we forget the private security guards who were just as brave, just as courageous, just as helpful, and ultimately just as self-sacrificing.

**Slide 24: Graph**

Some time about 1980, the reported numbers showed that private security had eclipsed public policing. As a result of national security concerns following the 9-11 attacks numbers were not reported and some public and some private roles were differently reported. We now benchmark private security as having three times the resources and personnel as public policing.

**Slide 25: The Worst Security**

Right now, today, the city police are under siege from the media and from assassins on the street. That said, supportive as we all are, they are not your security force.

**Slide 26: Supreme Court**

(No comment.)

**Slide 27: Superman**

You are enamored of your Constitutional rights, and rightfully so. However, at work, under the watchful eye of private security, you do not have those rights. We are not the police. We can search your car without a warrant. Under orders from corporate policy, we can prevent you from posting religious symbols. In other words, we are not limited to a defensive reaction to crime. We have the power needed to get above and beyond the evil perpetrators in order to protect you.
**Slide 29** When I work as a security guard my bachelors and masters degrees are not displayed on my uniform.

**Slide 30** I guarded with a Ph.D. professor of philosophy who was between jobs and re-evaluating his life.

**Slide 31**: I patrolled with a retired nuclear engineer.

**Slide 32** Two of my supervisors were degreed and ordained ministers.

**Slide 33** And 40% of us are former police or military.

**Slide 33.** The American Society for Industrial Security was re-branded to **ASIS International**. Yes, that is Steve Wozniak.

**Slide 34**: We will be in Dallas next year. I just want to say that I am not a member of ASIS. I have been, but I am not now currently. BTW in this screen shot, Dr. Jennifer Hesterman is a retired Air Force colonel.

**Slide 35: Certifications**

Information systems and computer security professionals are all about certifications. Do not... do not... do not... engage anyone to make chief security officer decisions who does not hold ASIS credentials. You get these yahoos who say, “I have 25 years of experience with the Houston Police Department.” Or “I was on the Drug Enforcement Task Force.” Or whatever. You already know that those are admissions of the failure mode. If you respect your own certifications, you will insist that your CSO holds ASIS credentials.

And BTW, I have none. I came into this late in life and I never had the required five years of experience in private security supervision and management necessary for the lowest level of certification from ASIS International.

**Slide 36: What Private Security Does**

You call the police after someone has harmed you. You contract with private security to prevent harms.

**Slide 37: Independence**

I am going to belabor this in the next few slides. Too often security is placed under facilities. The number one metric for facilities is cost. But with security, your safety has no price tag. More deeply, facilities managers
simply are not rewarded for protecting you. They keep you cool in the summer and warm in the winter, but if your abusive ex-partner violates a restraining order and beats you up in the parking lot, it is not their problem. If someone slips into the rack room and downloads all the customer data, it has nothing to do with facilities.

The reason that you want contract security guards is that you do not want them to have relationships with your staff. They have to have a different source for their paychecks in order to be able to hold everyone accountable.

**Slide 38: Assessments**

Your security manager – or a security firm seeking a contract – can deliver several invaluable reports. These are all known. Very few places on Earth, not Afghanistan or Iraq, not Austin or Round Rock, are so unusual that a security assessment would be a truly novel undertaking.

Moreover, I also work in emergency management through the Texas State Guard and I am member of AUSTIN CERT, the Community Emergency Response Team. We all speak in the same language of threats, risks, exposures, preventions, mitigations, responses and recoveries.

In short, this is known technology. You just have to actually do it.

**Slide 39: Site Assessments (2)**

Realize that your local police department will come out for free and inspect your locks and windows. It is worth the price. Beyond that, you need someone who can tell you when and whether the industrial spy can get in.

If you want a secure environment, you have to limit cell phones. Get everyone a desk phone. Make them check their cell phones in a locker when they come in.

At the Texas National Guard, USB drives are forbidden. I just point out that you can make and enforce any reasonable rule to protect your intellectual property and secure your environment.

**Slide 40 Site Assessment**
As we will see, the best way to attack this is from the viewpoint of a violator. You have to think like a criminal,...which for a hacker is all too easy. This is a Google Maps view of a mortgage bank that I guarded during the mortgage meltdown. The circles are doors. The problem for security was to figure out where the blind spots were. When the company was sold, the new owners installed more cameras. Cameras are pretty cheap, but so are some business owners.

**Slide 45: Access Control**
In order to keep intruders out, you need to define your perimeter. It begins farther out than you might at first think. In point of fact, if you design your facility well, it will begin about 100 meters farther out than you imagined it did. We all know that those big red concrete balls at Target are not for decoration. Your security people can recommend many different modes and features to secure your perimeter and your entries and exits.

**Slide 41: Guards Inspect Infrastructure**
Maybe you are pretty good as a penetrator and you have been here, but, myself up here on the roof or in a confined space, I never see a software guru looking for penetration points. Mostly, I see places no one wants to be.

Your guards on patrol know your facility intimately. Facilities workers fix things or prevent them from breaking. Most guards are pretty good at spotting the things that leave you unsafe as you blithely keyboard away in your cubie.

One time working in campus safety, over the holidays, I was on the fourth floor of a nominally three-story building and heard an alarm. I followed the sound and faced a large heater, a furnace behind a thick enclosure with a steel door. The door had a thick window. I called it in. The dispatcher told me to check it out. I said, “Is this not a facilities problem?” And the dispatcher informed me that facilities would not enter the boiler room until I said that it was safe. So, OK, I felt the door. It was not hot. I carefully opened the door, using it as a blast shield, waiting for the wall of flames. So, this time, it was OK. I called it in. 45 minutes later a facilities manager left his New Years Eve activities to come into work to check this out. Imagine what it would have been like if no one had responded and you came in on Monday morning and about 10 o’clock, the boiler exploded.
Slide 45: Auditable Controls
Work schedules and contact information should be posted in the ready room for the guards. They need to know who is working when, and how to contact their co-workers.

Visitor logs provide evidence after the fact, but, more importantly, those schedules let guards prepare access cards, badges, and other materials and just allow a preview of who they will be meeting and greeting.

I cannot stress education and training enough. It is an auditable control to demonstrate that your organization is mature and capable because you have methods in place to improve the processes. When I worked at Securitas and Allied Barton, I was assigned to complete online training and certification in about 20 areas from traffic control to fire fighting.

Slide 46: Dealer Program.

The tools you need are all easy to find. This is what the Pentagon calls COTS C-O-T-S: commercial off-the-shelf technology. Everyone in this room has more than the mere ability, but in fact a driving passion to get in where you are not wanted. That kind of thinking is fundamental to designing defenses and responses. It is a fact from cryptography that no one can design a secure system who has not made a career of breaking them.

Slide 46: Newton Man Trap.

E Pluribus Unum means “From Many, One” but I like to translate it as “One out of many” because I am not endorsing this brand, just pointing out that this is known technology. You can put them in every corridor with different kinds of codes. Computer people love this kind of gaming. You could have one with no codes and then catch the intruder who is busy trying to hack the system that does not need hacking.

Slide 48: Two Factor Authentication.
Nothing new here, but if you do not have it, then you have not even bothered to lock the front door. These machines are cheaper than massive data breaches.

But I do want to stress that we know in security that your perpetrators are about 20% more likely to come from the inside than from outside.
Assessing the sociology of your own workplace is the first step to securing your information assets against compromise or loss. But you still need to secure the outside.

**Slide 48: Keep a clear zone.**

This is why security cannot be subordinate to facilities. My boss wrote this up several times. I wrote it up several times. Nothing was done because the maintenance staff did not need to follow security directives. We had to follow theirs. They did not want to clean this up and we could not make them. Not only could an intruder jump the fence the pallet would be a good way to start a fire. The fire would distract everyone while the intruder entered from another side.

**Slide 50: Razor wire.** I took these pictures and the previous one while guarding a server farm here in Austin. I am sure that when the sales people walked the clients around, it was on the inside where all the fancy bells and whistles are. The potential clients did not inspect the perimeter with the hard eye of a security guard.

**Slide 52: The Red Team is so friendly…**

This is Jayson Street at BSides 2013. His talk “How Do I PWN thee, let me count the ways” was about his red hat physical penetrations. He was dismayed at how easy it was to get past security guards with some flimsy documentation. He claimed to have an email or fax from a corporate officer granting him access to fix something and he was allowed in. It was embarrassingly simple. I took all of his lessons back to work with me to alert my colleagues to the ways that we could fail. One thing I will say, though, is that every site I worked here in Austin for Securitas had active visitor logs. No one got in if they were not expected.

Jayson is talking to my wife, Laurel. Many of you know her. She is a security auditor.

**Slide 53: She didn’t see that coming!**

It is not a question of whether or not your security defenses will fail, but how you deal with the failure. What is your next move?
The End.