Editor's Comments

Welcome to the second issue of volume 4 of the Journal of Physical Security (JPS). This is the first time that we have published two issues in the same year. This issue contains papers about securing houses of worship, estimating explosive blast damage, the differences between threats and vulnerabilities, and emerging new security paradigms.

As usual, the views expressed in the Journal of Physical Security are those of the respective authors and should not necessarily be ascribed to Argonne National Laboratory or the United States Department of Energy.

There continues to be considerable enthusiasm for JPS on the part of the readership, but also a lot of trepidation among potential authors who are considering submitting manuscripts. (I know this because they often call me up with potential topics, worried about proceeding.) Authors who have published in JPS have found the process rewarding, have gained fresh insight into important security issues, and have educated a lot of readers on important security points. Please consider submitting a manuscript and encouraging colleagues and students to do likewise!

What follows are some rambling thoughts about physical security vs. cyber security, the importance of a stiff upper lip, patents and security, and how to spot Security Theater.

I gave the Keynote Address at the 19th Annual USENIX Conference in Washington, D.C. in August. (See http://www.youtube.com/watch?v=51MxGK2q7Wo) This was the first time I've attended USENIX. I was very favorably impressed with the quality of the presentations and the work they represent. I was also struck by how different the cyber security culture is from the physical security culture.

This difference greatly complicates the Convergence problem—also known as the "Thugs vs. Nerds" problem—which is the bringing together of physical and cyber security. Increasingly, good cyber security requires better physical security, and physical security practitioners find themselves working with software programs and with hardware devices that are interfaced to complex cyber networks and/or have substantial embedded computing or microprocessor power. Cyber vulnerabilities can quickly become physical security vulnerabilities, and vice versa.

Having moved around a bit in both worlds, here are my lists of what cyber security professionals and physical security professionals can potentially learn from each other:

What Physical Security Professionals Could Learn from Cyber Security Professionals

- Vulnerabilities are numerous, ubiquitous, inevitable, & constantly evolving.
- They don't automatically mean somebody has been screwing up.
- Scapegoating isn't very helpful.
- Security is not binary, it's a continuum.
- Customer focus: productivity has to be an issue in security.
- How to motivate good security practice among regular employees.
- Past criminals can make good consultants.
- Technology is not a panacea—security is really about people.
- Regular employees *are* the security, not the enemy of security.
- Lose the coat & tie!

What Cyber Security Professionals Could Learn from Physical Security Professionals

- Discipline, Leadership, Organizational Skills, & Being a Team Player.
- Understanding where you fit into the organization.
- Techniques for dealing with upper management; Making the business case for security.
- Effective project management & budgeting; meeting deadlines.
- Females can be very effective security professionals.
- Street smarts, people skills, & a good understanding of psychology.
- Dealing with Social Engineering & the Insider Threat.
- Realization that good cyber security requires good physical security.
- Maybe that T-shirt could be washed once in a while!

A recent article in the *Financial Times* (Page 17, September 5/5, 2010) got me thinking about 9/11. The article claims that, "Even at the height of the Blitz, Londoners were more bothered by the weather."

Most of the victims of the German bombing of England (the "Blitz") in World War II were civilians. A total of 43,683 people were killed by the Blitz in London alone by May of 1941. Many Londoners took shelter at night, including in the Underground.

Despite the bombings and the disruption to daily life they caused, a December 1940 survey of Londoners asked them to rank what most impacted their lives and their feelings. They ranked the "weather" first, "general war news" second, and "air raids" only third. This is surely an example of great courage and the famous British "stiff upper lip".

By comparison, the loss of 2,752 lives in New York on 9/11 due to murderous terrorists—as horrific as it was—involved much less loss of life. In fact, the following table lists various causes American deaths in 2001, most of which were preventable.

2001 Causes of American Deaths	Number
9/11 Terrorism	2,752
Drunk Driving	17,448
Not Wearing Seat Belts	19,146
Guns	29,573
Deaths Due to Smoking	428,000

The next table lists the approximate lifetime odds of an American dying of various causes. It shows that terrorism is not a very high risk factor.

Cause of Death	Lifetime Odds
Cancer	1 in 5
Automobile Crash	1 in 83
Suicide	1 in 119
Murder (not due to terrorism)	1 in 210
Walking Across the Street	1 in 625
Airplane Crash	1 in 5,000
Lightning	1 in 80,000
Terrorism	1 in 88,000

So, while it is true that (1) the cowardly and murderous acts of 9/11 are unacceptable, (2) they resulted in a terrible loss to the victims' families, (3) the animals responsible need to be hunted down, and (4) we need as effective a level of homeland security as is prudent, the obvious question is why did 9/11 change America? Terrorists win—even when nobody dies—when they generate fear, cause us to modify our lifestyle, and/or make us compromise our basic values and principles for an illusionary goal of absolute safety. Perhaps we could use more of the Brits' stiff upper lip.

I'm always amazed when manufacturers of security devices and systems tout the fact that their product is patented as if this was a good thing. By law, patents have to be fully enabling. Thus, while it may be entirely proper and prudent for a manufacturer to patent inventions, a patent is not a positive security attribute, it is a vulnerability. It explains (including to the bad guys and vulnerability assessors) how everything works.

Bruce Schneier coined the term "Security Theater" to describe the situation where phony security measures provide a feeling of improved security, but in reality provide little or no actual security. Another name for Security Theater is "Ceremonial Security".

As a vulnerability assessor, I frequently find Security Theater across a wide range of different physical security devices, systems, and programs, as well as in domestic and international nuclear safeguards. It's important to realize, however, that Security Theater is not automatically a bad thing. It can present the appearance (false though it may be) of a hardened target to potential adversaries, thus potentially discouraging an attack (at least for a while). Security Theater can reassure the public while more effective measures are under development, and help encourage employees and the public to take security seriously.

In international treaty monitoring and verification, Security Theater can help foster an environment of transparency, trust, confidence-building, and international cooperation. Security Theater can provide great photo opportunities for national leaders trying to promote disarmament regimes that may face intense political opposition. It can also serve as a first step in creating new regimes (because Security Theater is always easier than real security). During treaty negotiations, Security Theater can serve as an easy-to-negotiate stand-in for more rigorous security and safeguards procedures to be developed and negotiated in the future. Perhaps most importantly, Security Theater can provide an excuse to get inspectors inside nuclear facilities where their informal observations and interactions with host facility personnel can be of great value to disarmament, nonproliferation, and safeguards efforts.

The real problem occurs when Security Theater is not recognized as such, or when it stands in the way of good security or is actually preferred over real security (because it is easier).

The best way to spot Security Theater is to critically analyze the security it purports to offer. This, however, takes a lot of work. An easier way is to look for the attributes commonly found with Security Theater. The following is my list. If a third or more of these attributes reasonably apply to a given security device, system, measure, or program, it is likely to be Security Theater. The more the attributes apply, and the more of them that apply, the more likely you are looking at Security Theater, not real Security. (For more information, see RG Johnston and JS Warner, "Security Theater in Future Arms Control Regimes", *Proceedings of the 51st INMM Meeting*, Baltimore, MD, July 11-15, 2010.)

The Security Theater Attributes Model: The following are the typical attributes of technologies, measures, and procedures that are Security Theater. They are listed in no particular order.

1. There is great urgency to get something out in the field, or at least its acceptance negotiated.

2. The promoters and developers of the technology or procedure earnestly—even desperately—want it to solve the security or verification problems. (Strong proponents of nuclear disarmament and nonproliferation efforts often intensely wish, quite admirably, to make the world safe from nuclear hazards. This can sometimes lead to wishful thinking.)

3. There is considerable enthusiasm for, great pride in, and strong emotion behind the proposed (or fielded) technology or procedure.

4. The technology or procedure is a pet technology of the promoters and developers, not necessarily the technology or procedure that was chosen from among many candidates as a result of a careful study of the specific security/safeguards/verification problem of interest.

5. The security/safeguards/verification technology or procedure is viewed with great confidence, arrogance, and/or represented as "impossible defeat" or nearly so. (Effective security is very difficult to achieve. Generally, if promoters and developers of a given security or safeguards approach or hardware have carefully considered the real-world security issues, they will not be in such a boosterism mode. Fear is, in fact, a good indicator of a realistic mindset when it comes to security.)

6. There is a great deal of bureaucratic or political inertia behind the technology or procedure.

7. Substantial time, funding, and political capital has already been spent developing, promoting, or analyzing the technology or procedure.

8. The people or organization promoting the technology or procedure have a conflict of interest, or at least are unable to objectively evaluate it.

9. No vulnerability assessors, people with a "hacking" mentality, devil's advocates, or creative question-askers have closely examined the technology or procedure (perhaps because they weren't allowed to).

10. Anybody questioning the efficacy of the technology or procedure is ignored, attacked, ostracized, or retaliated against.

11. The people developing or promoting the technology or procedure have no real-world security experience.

12. The people developing or promoting the technology or procedure are mostly engineers. (No insult to engineers intended here. In our experience, the mindset and practices that makes one good at engineering aren't the optimal mindset for good security. Engineers tend to work in solution space, not problem space. They tend to view Nature and stochastic failures as the adversary, not maliciously evil people who attack intelligently and surreptitiously. They strive to design devices, hardware, and software that are user friendly, easy to service, and full of optional features—which tends to make attacks easier.)

13. Vulnerabilities are only considered, and vulnerability assessors only involved, after the development of the technology or procedure has been nearly completed. (At this point, it is usually too difficult to make necessary changes to improve the security for economic, political, timeliness, or psychological reasons).

14. The technology or procedure involves new technology piled on existing technology or

procedures in hopes of getting better security, but without actually addressing the Achilles heel of the old technology or procedure.

15. The technology or procedure relies primarily on complexity, advanced technology, the latest technological "fad", and/or multiple layers. (High technology does not equal high security, and layered security isn't always better.)

16. Any consideration of security issues focuses mostly on software or firmware attacks, not on physical security.

17. The main tamper detection mechanism—if there even is one—is a mechanical tamper switch or an adhesive label seal. (This is approximately the same, in our experience, as having no tamper detection at all.)

18. The technology or procedure is not directed against a specific, well-defined adversary with well-defined resources.

19. The end users of the technology or procedure have never been consulted and/or the technology or procedure is being forced on them from above. (These are people who understand the real-world implementation issues, and are the ones who will have to make the technology or procedure actually work).

20. The technology or procedure is not well understood by the non-technical people proposing or promoting it (or by the people in the field who are to use it), and/or the terminology being used is misleading, confusing, or ambiguous.

21. Particularly with security procedures: control or formalism gets confused with security.

22. Domestic and international nuclear safeguards get confused. (These two security applications are remarkably dissimilar.)

23. The technology or procedure in question makes people feel good. (In general, real security doesn't make people feel better, it makes them feel worse. This is because it is almost always more expensive, time-consuming, and painful than Security Theater. When security or safeguards are thoroughly thought-through, the difficulty of the task and knowledge of the unmitigated vulnerabilities will cause alarm. Fear is a good vaccine against both arrogance and ignorance.
This is the basis of what we call the "Be Afraid, Be Very Afraid Maxim": If you're not running scared, you have bad security or a bad security product.)

24. The use protocols for the technology or procedures are non-existent, vague, or ill-conceived.

25. The security application is exceeding difficult, and total security may not even be possible.

26. The terminology is vague, confusing, misleading, or full of wishful thinking, e.g., "high security", "tamper-proof", "pick proof", "undefeatable", "due diligence", "barrier", "certified",

"fully tested", "reliable", "real-time", "zero error rate", "unique", "industry leader", "industry standard", etc.

-- Roger Johnston, Argonne National Laboratory, September 2010