Keynote Address for *Security in Government Conference* (SIG 2011)
Canberra, Australia, July 25-27, 2011

A Cynical View of Security
(Or The Importance of Not Being Earnest)

Roger G. Johnston, Ph.D., CPP

Introduction

In an era when there has been substantial criticism—I think with some merit—of security measures not respecting civil liberties and privacy, how appropriate that we meet tonight in a house dedicated to working democracy, just meters away from the Magna Carta, an iconic symbol of individual rights and the rule of law.

20 years ago, I visited this very building and saw the Magna Carta, one of 4 surviving originals from 1297. A group of school children were visiting the Parliament House. While on their lunch break, they were running around the Magna Carta, throwing half-eaten sandwiches at each other. I thought, "How cool is that! And quintessentially Australian." In most places in the world, the Magna Carta would be mothballed in some stuffy museum. But here it was a living document.

Cynicism

Over 2 decades of doing vulnerability assessments on about 1000 different physical security (and nuclear safeguards) devices, systems, and programs, I've encountered many examples of arrogance, over-confidence, stupidity, and a lack of common sense, not to mention scapegoating, bureaucratic incompetence, wasted resources, Security Theater (ceremonial or fake security), denial and wishful thinking, hype and snake oil, mental laziness and sloppy thinking, deeply flawed security products, dumb hardware designs, dysfunctional security cultures, and highly counter-productive security rules.

Other than that, everything's been swell.

I don't think it is possible to have witnessed all of this and not be at least a bit cynical. In fact, most vulnerability assessors I know are pretty cynical. It just may be a hazard of the job.

Perhaps more importantly, though, I would argue that cynicism—or at least a hearty skepticism—is actually a very useful tool, not just an inevitable side effect. It

can, I believe, help professional vulnerability assessors, but also anybody wanting to critically examine their own security.

When you are cynical (or at least skeptical), you don't automatically buy into the hidden assumptions, the groupthink, or the wishful thinking too often associated with security. You're immune to the hype and the smoke and mirrors of pet or fad technologies. You're don't have the mental conflict of interest where you can't see security flaws because you—quite earnestly—don't want there to be security flaws.

Let's agree, though, that there are plenty of things in security not to be cynical about—especially now that our thoughts and prayers are with the good people of Norway. I've met innumerable hard working, dedicated security professionals; there's nothing to be cynical about there. And who could be cynical about the courage and self-sacrifice of police officers, firefighters, front-line security officers, emergency responders, and our heroic men and women serving in the military?

What is a Cynic?

Dictionaries: A person with an attitude of scornful or jaded negativity. (In my view, this is a rather cynical definition!)

Someone who puts all human actions into two classes — openly bad and secretly bad.
-- Henry Ward Beecher (1813-1887)

One who not only reads bitter lessons from the past, but also is prematurely disappointed in the future.
-- Sidney J. Harris (1917-1986)

An idealist whose rose-colored glasses have been removed, snapped in two, and stomped into the ground, immediately improving his vision.
-- Rick Bayan

A person with the power of accurate observation, labeled a cynic by those without it.
-- George Bernard Shaw (1856-1950)

A person who has an unpleasant way of saying the truth.
-- Lillian Hellman (1905-1984)

A cynic is a disappointed idealist.
-- George Carlin (1937-2008)

A person who knows the price of everything and the value of nothing.
-- Oscar Wilde (1854-1900) from *Lady Windermere's Fan*

Oscar Wilde

I'd like to briefly focus on Oscar Wilde (1854-1900) because I think he serves as an excellent prototype for a vulnerability assessor, or indeed for anyone trying to critically evaluate her security.

Wilde had many of the same attributes we see in modern-day hackers, vulnerability assessors, and inside attackers: self-reliance; narcissism; confidence in his intelligence and ability to find fault and challenge assumptions; a powerful need for recognition and to be seen as clever; and a tendency to be highly unimpressed with authority, experts, bureaucrats, precedence, institutions, convention, and regulations.

Now Oscar Wilde wasn't interested in security, though maybe he should have been. His 2-year lecture tour of North America in 1882 resulted in some near riots—fairly amazing given that he was lecturing on things like English poetry and the importance of the decorative arts. He was also cheated at the game of Bunco ("Eight Dice Cloth") while in the U.S. And as a student at Oxford, he single-handedly thrashed 4 students who physically attacked him.

Though not interested in security, Wilde was a kind of vulnerability assessor of art and literature, and especially of Victorian society. He felt that Victorian society was too focused on the trivial, too destructive of the individual, and not sufficiently sincere about important things, including the arts, esthetics, and learning.

Probably Wilde's most beloved play is the "The Importance of Being Earnest", a comedy of errors which, as many critics have pointed out, is really about the importance of NOT being earnest. The play, which mocks Victorian society, is about two men who pretend to be named "Earnest" as a ruse for bypassing social norms.

Wilde had plans to visit Australia but never followed through on them. To its credit, Australia (unlike England) did not ban his plays as a result of his scandalous reputation. Australian newspapers around 1895 warned their readers that Wilde was of dubious moral character, but that his plays were simply too good to suppress. A very modern attitude.

Oscar Wilde Quotations

Here are some quotations from Oscar Wilde's innovative essay, *The Critic as Artist*, which can almost be viewed as a guidebook for vulnerability assessors (though that is not what he had in mind):

"A little sincerity is a dangerous thing, and a great deal of it is absolutely fatal."

Very, very true about security! We need to stay cynical! If you're trying to think like the bad guys, you can't be sincere because they are usually not sincere.

"Man is least himself when he talks in his own person. Give him a mask, and he will tell you the truth."

Very much a Method Acting concept, though Method Acting was 3 decades in the future. The relevance to security: To think like the bad guys, don't be yourself!

"…a man cannot do a thing that he is the proper judge of it."

Thus, the importance of independent review of your security.

"It is always with the best intentions that the worst work is done."

This is definitely true about security!

Dumb Things in Security

In support of my cynical view of security, I offer you a very small sample of REALLY DUMB THINGS IN SECURITY from a giant universe of dumb things in security.

Let's be clear, though. The point is not to make fun of people and feel superior. That's just a fringe benefit. Our purpose here is to recognize that there really is a lot of fuzzy thinking in security, and to try to avoid it.

Let's start with U.S. homeland security, which in terms of identifying dumb things, is like shooting fish in a barrel.

<u>Homeland Security</u>

1. Nail clippers were seized from passengers by airport screeners after 9/11, presumably to prevent would-be hijackers from threatening the pilot with a bad manicure.

2. TSA Fires an Agent for Being a Witch (March 2011)
The Transportation Security Administration (TSA) at the Albany (New York) International Airport fired a security screener for being a witch. A fellow worker

accused the security screener, who practices Wicca, of casting a spell on her (the fellow worker's) car heater so that it wouldn't work.

Now...Lord knows that when we're on a witch hunt, we certainly don't want to be distracted by real witches!

3. In 2009, the United States decided to go stealth. A giant sign facing Canada was removed from the border station at Massena, NY for security reasons. The sign had 7-meter tall, screaming yellow letters spelling out "United States". According to a Department of Homeland Security official, "The sign could be a huge target and attract undue attention."

We probably should just rename the United States, "New Canada", thereby confusing both terrorists and Canadians. (The latter has no security implications, it's just fun.) I suppose Australia could similarly try to go stealth and change its geographical names, but frankly, you've got a lot of oddly named towns already, so I think it's probably confusing enough.

4. National Monuments that an infamous Department of Homeland Security memo listed as likely targets of terrorist attacks, and the funding allocated to prevent them:

- The Giant Lava Lamp, Soap Lake, Washington ($143 million)
- Carhenge, Alliance, Nebraska ($25 million)
- The World's Largest Ball of Paint, Alexandria, Indiana ($12 million)
- The Museum of Bad Art, Dedham, Massachusetts ($31 million)
- Barney Smith's Toilet Seat Art Museum, Alamo Heights, Texas ($10 million)

Icons of Western Civilization all!

My concern is whether Australia is spending the hundreds of millions of dollars needed to defend its icons. I'm referring, in particular, to the 150 or so Big Things—the giant roadside attractions such as the Big Banana, the Big Lobster, the Giant Murray Cod, or the Big Captain Cook.

The loss of something as iconic as the Big Boxing Crocodile would surely make it hard to go on!

Seals

Tamper-indicating seals are an area of particular silliness, perhaps because people are rather confused about tamper detection in general.

(tamper-indicating) seal: a device or material that leaves behind evidence of unauthorized entry (but doesn't attempt to prevent it, like a lock.) Most people are familiar with seals primarily in the context of tamper-evident packaging.

Some of the dumb things:

- Seals users who "know" their seals cannot be spoofed because they are called "tamper-proof" by the sales guy. Actually, the term makes no sense, nor does "tamper-resistant" (which is what a lock does).
- On a food product, printed on the seal and only on the seal: "Do not eat if seal is missing".
- ASKED FOR: A seal you don't have to inspect.
- ASKED FOR: A frangible (brittle) adhesive label seal that can be reused to save money.
- ASKED FOR: An adhesive label seal that is IMPOSSIBLE for the bad guys to remove, but when we remove it, no adhesive residue is left behind on the surface.
- Sealing (or locking) a container or room with the hinges on the outside.
- Sealing (or locking) a container with a giant hole in it.
- "high security" seals in ISO 17712
- My favorite: The cable tie as a "seal"—no serial number, cheap and widely available, easily picked open.

Security Maxims

As a result of my hard-earned cynicism, I've compiled a list of about 120 (slightly cynical) Security Maxims, a few of which I discuss here. These rules of thumb aren't absolute theorems or laws, but in my experience, they are true about 80-90% of the time in physical security or nuclear safeguards, and probably have some validity for cyber security.

Unfortunately in security, the bad guys get to define the problem, not the good guys, but you would never know it from the way most security is designed and analyzed.

Thus, the "I am Spartacus Maxim": Most vulnerability or risk assessments will let the good guys (and the existing security infrastructure, hardware, and strategies) define the problem, in contrast to real-world security applications where the bad guys get to. [Named for the catch-phrase from the 1960 Stanley Kubrick film "Spartacus". When the Romans captured Spartacus's army, they demanded he identify himself, but all his soldiers claimed to be Spartacus. Not historically realistic but very Hollywood! (But are the Romans the good guys or the bad guys here?)]

High-Tech Maxim: The amount of careful thinking that has gone into a given security device, system, or program is inversely proportional to the amount of high-

technology it uses. Comment: High-technology is often taken as a license to stop thinking critically. And in my experience, high-tech security products and programs are often remarkably easy to defeat with primitive attack methods.

You Must Be High Maxim: Any security product that is labeled "high security" isn't.

Depth, What Depth? Maxim: For any given security program, the amount of careful thinking that has been undertaken is inversely proportional to how strongly the strategy of "Security in Depth" (layered security) is invoked. Comment: It's not that layered security is wrong, it's just that it often becomes an excuse to stop thinking critically about security.

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time. [So you had better factor this into security planning. Named in honor of Hans Rohrbach (1903-1993), the German mathematician and cipher expert.]

Rohrbach Was An Optimist Maxim: No security device, system, or program will ever be used properly.

Show Me Maxim: No serious security vulnerability, including blatantly obvious ones, will be dealt with until there is overwhelming evidence and widespread recognition that adversaries have already catastrophically exploited it.

Somebody Must've Thought It Through Maxim: The more important the security application, the less careful and critical thought and research has gone into it. [I would claim that the security of soda vending machine and also of blackjack games at casinos has been much more carefully thought through than homeland security, nuclear safeguards (especially international safeguards), or election integrity.]

Mahbubani's (or the Titanic) Maxim: Organizations and security managers who cannot envision security failures, will not be able to avoid them. (Named for Kishore Mahbubani, scholar and diplomat.)

I like Dan Philpott's comment that: "Sometimes security implementations look fool proof. And by that, I mean proof that fools exist."

He Who's Name Must Never Be Spoken Maxim: Security programs and professionals who don't talk a lot about "the adversary" or the "bad guys" aren't prepared for them and don't have good security. (From the Harry Potter books.)

Speaking of Harry Potter, I can certainly sympathize with the exasperated caller to a BBC Radio show in the UK. "Harry Potter this, Harry Potter that!" she said, "I'd never even heard of Harry Potter until that book came out!"

So We're In Agreement Maxim: If you're happy with your security, so are the bad guys.

Feynman's Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security improvements more than malicious adversaries. [There's a lot of 'shoot the messenger' in the vulnerability assessment business.]

Scapegoat Maxim: The main purpose of an official inquiry after a serious security incident is to find somebody to blame, not to fix the problems.

Alice Springs Maxim: One-size-fits-all will be greatly preferred for security because it requires less thinking. Organizations will be loath to factor in local, on-the-ground details. [This maxim is so named because of the advice sometimes given to scared tourists about their being relatively few shark attacks in Alice Springs.]

If you're interested in more of our Security Maxims, they can be found at http://www.ne.anl.gov/capabilities/vat/seals/maxims.shtml.

Criticism is Easy, But What Are Some of the Things We Can Do Better?

- ✓ More cynicism (or at least skepticism) and critical thinking.
- ✓ Less prevention, more mitigation and resilience, especially for terrorism.
- ✓ Be proactive to the Insider Threat—including educating employees about social engineering and practicing effective disgruntlement mitigation.
- ✓ Try bribes! Being from Chicago, I am a big believer in bribing people! Test your people's loyalty, then let them keep the money if they reject the bribe to do nefarious deeds, and make them organizational heroes. This efficiently sends the message it would be a good idea to turn down bribes. (There are legal entrapment issues, but firing or arresting people is not the point here.)
- ✓ Put up posters with eyes. See, for example, *Biology Letters* **2**, 412-414 (2006): http://rsbl.royalsocietypublishing.org/content/2/3/412.full
- ✓ Embrace the new security paradigms:

Old Paradigm	New Paradigm
Security is easy & binary.	It's not. It's a continuum with lots of difficult trade-offs.
Vulnerabilities are bad news.	Vulnerabilities are good news. They are always present in large numbers. When we find one, we can do something about it.
There is one right answer. We seek accountability and good security through fear, scapegoating, threatening, & firing people.	We embrace creativity, flexibility, uncertainty, criticism, questions, and dissent. As George S. Patton said, "when everybody is thinking alike, nobody is thinking". Security should be controversial. We watch for the dangers of cognitive dissonance. We motivate & encourage good security practice.
Compliance-based security: Security is about knowing and following the rules. Security gets confused with Control, Big Brother, and Security Theater.	We strive for thinking-based security, not compliance-based. We must do more than mere compliance. Sometimes we must pushback against compliance when it is Security Theater or interferes with Security or Productivity or Privacy. Security cannot be the enemy of employees or the public! Lots of "what if?" exercises, lots of emphasis on being proactive, creative, and showing individual initiative.
Security by Obscurity (trying to keep secrets)	Transparency in many things—allowing criticism, improvement, and accountability.
Security Professionals provide security.	The Insider Threat not withstanding, citizens, employees, contractors, vendors, customers, and visitors provide security. Security Professionals help.

Conclusion

Let me conclude with a little wisdom from comedienne Gracie Allen (1895-1964). She said she had been watching a lot of game shows on television. And she had come to realize that the people with the answers come and go, but the man with the questions has a permanent job.

My advice is to be the person asking the skeptical or cynical questions about security. Don't be the one who presumes to have the definitive answers. Security is difficult.