

Physical Security Maxims

Argonne Vulnerability Assessment Team
Roger G. Johnston, Ph.D., CPP
rogerj@anl.gov, 630-252-6168

Last Updated: December 23, 2008

The following maxims are somewhat cynical and tongue-in-cheek. Nevertheless they say important things about physical security, and are essentially correct 80-90% of the time (unfortunately).

Physical Security Maxims by Roger G. Johnston | Last Updated: December 23, 2008

Infinity Maxim: There are an unlimited number of security vulnerabilities for a given security device, system, or program, most of which will never be discovered (by the good guys or bad guys).

Arrogance Maxim: The ease of defeating a security device or system is proportional to how confident/arrogant the designer, manufacturer, or user is about it, and to how often they use words like “impossible” or “tamper-proof”.

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it.

Be Afraid, Be Very Afraid Maxim: If you’re not running scared, you have bad security or a bad security product.

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.

Schneier’s Maxim #1: The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems.

Schneier’s Maxim #2: Control will usually get confused with Security.

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems).

Father Knows Best Maxim: The amount that (non-security) senior managers in any organization know about security is inversely proportional to (1) how easy they think security is, and (2) how much they will micro-manage security and invent arbitrary rules.

Huh Maxim: When a (non-security) senior manager, bureaucrat, or government official talks publicly about security, he or she will usually say something stupid, unrealistic, inaccurate, and/or naïve.

Voltaire’s Maxim: The problem with common sense is that it is not all that common.

Physical Security Maxims by Roger G. Johnston | Last Updated: December 23, 2008

Yipee Maxim: There are effective, simple, & low-cost counter- measures (at least partial countermeasures) to most vulnerabilities.

Arg Maxim: But users, manufacturers, managers, & bureaucrats will be reluctant to implement them for reasons of inertia, pride, bureaucracy, fear, wishful thinking, and/or cognitive dissonance.

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. In other words, “significant psychological (or literal) damage is required before any significant security changes will be made”.

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells security products or services is prepared to answer a significant question about vulnerabilities, and few potential customers will ever ask them one.

Bob Knows a Guy Maxim: Most security products and services will be chosen by the end-user based on purchase price plus hype, rumor, innuendo, hearsay, and gossip.

Familiarity Maxim: Any security technology becomes more vulnerable to attacks when it becomes more widely used, and when it has been used for a longer period of time.

Antique Maxim: A security device, system, or program is most vulnerable near the end of its life.

Payoff Maxim: The more money that can be made from defeating a technology, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 1: The more a given technology is despised or distrusted, the more attacks, attackers, and hackers will appear.

I Hate You Maxim 2: The more a given technology causes hassles or annoys security personnel, the less effective it will be.

Shannon’s (Kerckhoffs’) Maxim: The adversaries know and understand the security hardware and strategies being employed.

Corollary to Shannon’s Maxim: Thus, “Security by Obscurity”, i.e., security based on keeping long-term secrets, is not a good idea.

Gossip Maxim: People and organizations can’t keep secrets.

Plug into the Formula Maxim: Engineers don’t understand security. They think nature is the adversary, not people. They tend to work in solution space, not problem space. They think systems fail stochastically, not through intelligent malicious intent.

Physical Security Maxims by Roger G. Johnston | Last Updated: December 23, 2008

Rohrbach's Maxim: No security device, system, or program will ever be used properly (the way it was designed) all the time.

Rohrbach Was An Optimist Maxim: Few security devices, systems, or programs will ever be used properly.

Insider Risk Maxim: Most organizations will ignore or seriously underestimate the threat from insiders.

We Have Met the Enemy and He is Us Maxim: The insider threat from careless or complacent employees & contractors exceeds the threat from malicious insiders (though the latter is not negligible.)

Troublemaker Maxim: The probability that a security professional has been marginalized by his or her organization is proportional to his/her skill, creativity, knowledge, competence, and eagerness to provide effective security.

Feynman's Maxim: An organization will fear and despise loyal vulnerability assessors and others who point out vulnerabilities or suggest security changes more than malicious adversaries.

Irresponsibility Maxim: It'll often be considered "irresponsible" to point out security vulnerabilities (including the theoretical possibility that they might exist), but you'll rarely be called irresponsible for ignoring or covering them up.

Backwards Maxim: Most people will assume everything is secure until provided strong evidence to the contrary--exactly backwards from a reasonable approach.

You Could've Knocked Me Over with a Feather Maxim 1: Security managers, manufacturers, vendors, and end users will always be amazed at how easily their security products or programs can be defeated.

You Could've Knocked Me Over with a Feather Maxim 2: Having been amazed once, security managers, manufacturers, vendors, and end users will be equally amazed the next time around.

That's Why They Pay Us the Big Bucks Maxim: Security is nigh near impossible. It's extremely difficult to stop a determined adversary. Often the best you can do is discourage him, and maybe minimize the consequences when he does attack.

Throw the Bums Out Maxim: An organization that fires high-level security managers when there is a major security incident, or severely disciplines or fires low-level security personnel when there is a minor incident, will never have good security.

Physical Security Maxims by Roger G. Johnston | Last Updated: December 23, 2008

Better to be Lucky than Good Maxim: Most of the time when security appears to be working, it's because no adversary is currently prepared to attack.

A Priest, a Minister, and a Rabbi Maxim: People lacking imagination, skepticism, and a sense of humor should not work in the security field.

Mr. Spock Maxim: The effectiveness of a security device, system, or program is inversely proportional to how angry or upset people get about the idea that there might be vulnerabilities.

Double Edge Sword Maxim: Within a few months of its availability, new technology helps the bad guys at least as much as it helps the good guys.

Mission Creep Maxim: Any given device, system, or program that is designed for inventory will very quickly come to be viewed--quite incorrectly--as a security device, system, or program.

We'll Worry About it Later Maxim: Effective security is difficult enough when you design it in from first principles. It almost never works to retrofit it in, or to slap security on at the last minute, especially onto inventory technology.

Somebody Must've Thought It Through Maxim: The more important the security application, the less careful and critical thought has gone into it.

That's Entertainment Maxim: Ceremonial Security (a.k.a. "Security Theater") will usually be confused with Real Security; even when it is not, it will be favored over Real Security.

Ass Sets Maxim: Most security programs focus on protecting the wrong assets.

Vulnerabilities Trump Threats Maxim: If you know the vulnerabilities (weaknesses), you've got a shot at understanding the threats (the probability that the weaknesses will be exploited and by whom). Plus you might even be ok if you get the threats all wrong. But if you focus only on the threats, you're probably in trouble.

Mermaid Maxim: The most common excuse for not fixing security vulnerabilities is that they simply can't exist.

Onion Maxim: The second most common excuse for not fixing security vulnerabilities is that "we have many layers of security", i.e., we rely on "Security in Depth".

Hopeless Maxim: The third most common excuse for not fixing security vulnerabilities is that "all security devices, systems, and programs can be defeated". (This is typically expressed by the same person who initially invoked the Mermaid Maxim.)

Takes One to Know One: The fourth most common excuse for not fixing security vulnerabilities is that "our adversaries are too stupid and/or unresourceful to figure that out."

Physical Security Maxims by Roger G. Johnston | Last Updated: December 23, 2008

Depth, What Depth? Maxim: For any given security program, the amount of critical, skeptical, and intelligent thinking that has been undertaken is inversely proportional to how strongly the strategy of "Security in Depth" (layered security) is embraced.

Tabor Maxim #1: Security is an illusionary ideal created by people who have an overvalued sense of their own self worth.

Tabor Maxim #2: Security is practically achieved by making the cost of obtaining or damaging an asset higher than the value of the asset itself.

Buffett Maxim: You should only use security hardware, software, and strategies you understand.

Just Walk It Off Maxim: Most organizations will become so focused on prevention (which is very difficult at best), that they fail to adequately plan for mitigating attacks, and for recovering when attacks occur.

Thursday Maxim: Organizations and security managers will tend to automatically invoke irrational or fanciful reasons for claiming that they are immune to any postulated or demonstrated attack. (So named because if the attack was demonstrated on a Tuesday, it won't be viewed as applicable on Thursday.)

Galileo's Maxim: The more important the assets being guarded, or the more vulnerable the security program, the less willing its security managers will be to hear about vulnerabilities.

Michener's Maxim: We are never prepared for what we expect.

Accountability 1 Maxim: Organizations that talk a lot about holding people accountable for security are talking about mindless retaliation, not a sophisticated approach to motivating good security practices by trying to understand human and organizational psychology, and the realities of the workplace.

Accountability 2 Maxim: Organizations that talk a lot about holding people accountable for security will never have good security.

Blind-Sided Maxim: Organizations will usually be totally unprepared for the security implications of new technology, and the first impulse will be to try to mindlessly ban it.

Success Maxim: Most security programs "succeed" (in the sense of their being no apparent major security incidents) not on their merits but for one of these reasons: (1) the attack was surreptitious and has not yet been detected, (2) the attack was covered up by insiders afraid of retaliation and is not yet widely known, (3) the bad guys are currently inept but that will change, or (4) there are currently no bad guys interested in exploiting the vulnerabilities, either because other targets are more tempting or because bad guys are actually fairly rare.

Physical Security Maxims by Roger G. Johnston | Last Updated: December 23, 2008

Dr. Who Maxim: “The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious.”

Big Heads Maxim: The farther up the chain of command a (non-security) manager can be found, the more likely he or she thinks that (1) they understand security and (2) security is easy.