Security Maxims (Aug 2018)

Roger G. Johnston, Ph.D., CPP

Right Brain Sekurity (http://rbsekurity.com)

While these security maxims are not theorems or absolute truths, they are in my experience essentially valid 80-90% of the time in physical security and nuclear safeguards. They probably also have considerable applicability to cyber security.

Note that some of these maxims are obviously hyperbole and/or tongue-in-cheek, but that does not necessarily make them untrue. You ignore these maxims at your own (and others') peril, especially the ones in red!

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".

Warner's (Chinese Proverb) Maxim: There is only one beautiful baby in the world, and every mother has it. Comment: Everybody's security or security product is beautiful (to them).

Band Aid (Bolt On) Maxim: If a security device, system, or product isn't designed from the beginning with security in mind, it will never be secure. Comment: Security is something you have to design in, not add on as an afterthought via a "band aid" or "bolt on" approach.

Get Use To It Maxim: The recommended use protocol for any given security device, system, or product (if there even is one) is not well thought through from a vulnerability standpoint.

Be Afraid, Be Very Afraid Maxim: If you're not running scared, you have bad security or a bad security product. Comment: Fear is a good vaccine against both arrogance and ignorance.

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

Ignorance is Bliss Maxim: The confidence that people have in security is inversely proportional to how much they know about it. Comment: Security looks easy if you've never taken the time to think carefully about it.

Titanic Maxim: All confidence is over-confidence, if not arrogance.

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). Comment: We think this is true because we always find new vulnerabilities when we look at the same security device, system, or program a second or third time, and because we always find vulnerabilities that others miss, and vice versa.

Thanks for Nothin' Maxim: A vulnerability assessment that finds no vulnerabilities or only a few is worthless and wrong.

Weakest Link Maxim: The efficacy of security is determined more by what is done wrong than by what is done right. Comment: Because the bad guys typically attack deliberately and intelligently, not randomly.

Safety Maxim: Applying the methods of safety to security doesn't work well, but the reverse may have some merit. Comment: Safety is typically analyzed as a stochastic or event/fault tree kind of problem, whereas the bad guys typically attack deliberately and intelligently, not randomly. For a discussion about using security methods to improve safety, see RG Johnston, *Journal of Safety Research* **35**, 245-248 (2004).

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: In security, high-technology is often taken as a license to stop thinking critically.

Doctor Who Maxim: "The more sophisticated the technology, the more vulnerable it is to primitive attack. People often overlook the obvious." Comment: This quote is from Tom Baker as Doctor Who in *The Pirate Planet* (1978).

Low-Tech Maxim: Low-tech attacks work (even against high-tech devices and systems). Comment: So don't get too worked up about high-tech attacks.

Schneier's Maxim #1 (Don't Wet Your Pants Maxim): The more excited people are about a given security technology, the less they understand (1) that technology and (2) their own security problems. Comment: From security guru Bruce Schneier.

Sexy Maxim: The sexier a security device, system, or program appears to be, the less security it has to offer.

What a Deal Maxim: The introduction of high-tech security products into your security program will: (1) probably not improve your security, (2) almost certainly increase your overall security costs (though perhaps it will decrease inventory, shipping, or other business costs), and (3) probably increase security labor costs (with the sometimes exception of CCTV).

Too Good Maxim: If a given security product, technology, vendor, or techniques sounds too good to be true, it is. And it probably sucks big time.

You Must Be High Maxim 1: Any security product that is labeled "high security" isn't.

You Must Be High Maxim 2: "High Security" is a context- and application-dependent value judgment, not a product attribute.

That's Extra Maxim: Any given security product is unlikely to have significant security built in, and will thus be relatively easy to defeat.

I Just Work Here Maxim: No salesperson, engineer, or executive of a company that sells or designs 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.

My Crazy Girlfriend/Boyfriend Maxim: Any methodology for selecting a security device or system (or for deciding whether a new one should be fielded) will ignore, assign insufficient weight to, or be ignorant of the fact that it can be easily defeated. Consequently, the device or system will be accepted for reasons other than effective security. Comment: (Named after people who select a romantic partner with many admirable traits but who happen to be a psychopath.) If a security device or system does not provide good security, any of its other attributes are irrelevant. The maxim applies to qualitative, semi-quantitative, and quantitative methodologies for ranking/rating.

He Just Seems So Knowledgeable Maxim: Most organizations get the majority of their physical security advice from salespeople (who somehow seem to recommend their own products).

Tamper-Proof Maxim: Any claim by a salesperson about the performance of a physical security product (including the claim of absolute security) will be believed by default by the customer, while warnings about vulnerabilities or limitations by vulnerability assessors or others with first-hand experience will be met with incredulity. Comment: A classic example of this can be found in the all-to-common seal customers who maintain that their seals cannot not be spoofed because the manufacturer calls them "tamper-proof".

Magic Light Inside the Refrigerator Maxim: Deploying a simple mechanical tamper switch or light sensor to detect tampering with a device or container is approximately the same thing as having no tamper detection at all.

Key Maxim (Tobias's Maxim #1): The key does not unlock the lock. Comment: From Marc Weber Tobias. The point is that the key activates a mechanism that unlocks the lock. The bad guys can go directly to that central unlocking mechanism to attack the lock (or do other things) and entirely bypass the key or pins. This maxim is related to the "I am Spartacus Maxim" below and to a corollary (also from Marc Weber Tobias) that "electrons don't open doors, mechanical mechanisms do".

Tobias's Maxim #2: Things are rarely what they appear to be. Comment: From Marc Weber Tobias. Or as Yogi Berra said, "Nothing is like it seems, but everything is exactly like it is."

There's The Opening Maxim (Tobias's Maxim #3): Any opening in a security product creates a vulnerability. Comment: From Marc Weber Tobias.

Tobias's Maxim #4: You must carefully examine both critical and non-critical components to understand security. Comment: From Marc Weber Tobias.

Contrived Duelism/Dualism Maxim: The promoters of any security product meant to deal with any sufficiently challenging security problem will invoke a logical fallacy (called "Contrived Dualism") where only 2 alternatives are presented and we are pressured into making a choice, even though there are actually other possibilities. Comment: For example: "We found a convicted felon, gave him a crowbar, and he couldn't make the lock open after whaling on it for 10 minutes. Therefore, the lock is secure." Another example, "Nobody in the company that manufacturers this product can figure out how to defeat it, and I bet you, Mr./Ms. Potential Customer [never having seen this product before in your life] can't think up a viable attack on the spot. Therefore, this product is secure."

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.

Schneier's Maxim #2 (Control Freaks Maxim): Control will usually get confused with Security. Comment: From security guru Bruce Schneier. Even when Control doesn't get confused with Security, lots of people and organizations will use Security as an excuse to grab Control, e.g., the Patriot Act.

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.

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.

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. Comment: Real world security blunders are often stunningly dumb.

Yippee 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".

Friedman's Maxim: "Only a crisis—actual or perceived—produces real change. When the crisis occurs, the actions that are taken depend on the ideas that are lying around." --Milton Friedman (1912-2006). Comment: This is why it is so important to actively discuss and analyze alternative approaches to security. Not because they will be automatically adapted even if they are good ideas, but because we want lots of good ideas lying around for when a real or perceived serious security incident occurs.

Could've, Would've, Should've Maxim: Security Managers will dismiss a serious vulnerability as of no consequence if there exists a simple countermeasure—even if they haven't bothered to actually implement that countermeasure.

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.

Colsch's (KISS or Kitchen Sink) Maxim: Security won't work if there are too many different security measures to manage, and/or they are too complicated or hard to use.

That's Cold Maxim: An adversary who attacks cold (without advance knowledge or preparation) is stupid and amateurish, often too much so to be a real threat. Moreover, he almost never has to attack cold. Comment: Thus don't overly focus on this kind of attack, or use it as an excuse not to fix vulnerabilities.

Shannon's (Kerckhoffs') Maxim: The adversaries know and understand the security hardware, software, algorithms, and strategies being employed. Comment: This is one of the reasons why open source security (e.g., open source cryptography) makes sense.

Corollary to Shannon's Maxim: Thus, "Security by Obscurity", i.e., security based on keeping long-term secrets, is not a good idea. Comment: Short-term secrets can create useful uncertainty for an adversary, such as temporary passwords and unpredictable schedules for guard rounds. But relying on long term secrets is not smart. Ironically—and somewhat counter-intuitively—security is usually more effective when it is transparent. This allows for discussion, analysis, understanding, outside review, criticism, accountability, buy-in, and improvement.

Gossip Maxim: People and organizations can't keep secrets. Comment: See Manning and Snowden.

How Inconvenient! Maxim: Convenience is typically not compatible with good security, yet, paradoxically, security that isn't convenient usually doesn't work well.

Plug into the Formula Maxim: Engineers don't understand security. They tend to work in solution space, not problem space. They rely on conventional designs and focus on a good experience for the user and manufacturer, rather than a bad experience for the bad guy. They view nature or economics as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent. Being intelligent does not automatically make you think like a bad guy. (Magicians and con artists know that technical people are often the easiest people to scam because they think logically!)

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: No security device, system, or program will ever be used properly.

Ox Votes for the Moron Maxim: "Election Security" is an oxymoron.

Election Oaf Ficial Maxim: Any given election official most likely (1) doesn't believe that security is part of their job, (2) doesn't think there are any election security issues, and (3) has never tried to envision an attack.

Insider Risk Maxim: Most organizations will ignore or seriously underestimate the threat from insiders. Comment: Maybe from a combination of denial that we've hired bad people, and a (justifiable) fear of how hard it is to deal with the insider threat?

We Have Met the Enemy and He is Us Maxim: The insider threat from careless or complacent employees and contractors exceeds the threat from malicious insiders (though the latter is not negligible.) Comment: This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders. Also, see Schryver's Law below.

Fair Thee Well Maxim: Employers who talk a lot about treating employees fairly typically treat employees neither fairly nor (more importantly) well, thus aggravating the insider threat and employee turnover (which is also bad for security).

The Inmates are Happy Maxim: Large organizations and senior managers will go to great lengths to deny employee disgruntlement, see it as an insider threat, or do anything about it. Comment: There are a wide range of well-established tools for mitigating disgruntlement. Most are quite inexpensive.

Two Kinds Maxim 1: Disengaged employees fall into 2 categories, those who quit and leave, and those who quit and stay.

Two Kinds Maxim 2: Disgruntled employees fall into 2 categories, those who engage in retaliation & sabotage, and those who are currently contemplating it.

Make 'Em Gruntled Maxim: Disgruntlement is the easiest motivator of inside attackers to counter. Comment: There are a number of motivations for deliberate inside attacks. These include: greed; ideology, political activism, and radicalization; terrorism; coercion/ blackmail; desire for excitement; the phenomenon of a self-identified Cassandra; disgruntlement; and (maybe) mental illness. Of these, disgruntlement is the easiest to counter by treating insiders well, followed by dealing with Cassandras. [In Greek mythology, Cassandra was given the power of prophecy, but then cursed such that nobody would believe her. A self-identified Cassandra warns of security risks, but when isn't believed will instigate the prophesized attack(s).]

80% Maxim: When an employee is disgruntled, if someone in the organization with even a little authority will simply listen to, validate, and empathize with the employee, approximately 80% of the time the employee will feel significantly better about the problem, himself/herself, and the organization as a whole. Comment: Remarkably, it isn't even necessary to agree with the employee about their complaint(s), or fix whatever is bugging him or her—though, when possible, a sincere attempt to fix the problem can go a long ways towards mitigating the disgruntlement.

HR Maxim: In any given large organization, the Human Resources Department is more likely to make security worse than it is to make it better. Indeed, your greatest security threat may be HR.

Beef Jerky Maxim: Employees don't leave jobs, they leave jerks.

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. Comment: An entertaining example of this common phenomenon can be

found in "Surely You are Joking, Mr. Feynman!", published by W.W. Norton, 1997. During the Manhattan Project, when physicist Richard Feynman pointed out physical security vulnerabilities, he was banned from the facility, rather than having the vulnerability dealt with (which would have been easy).

Questionable Security Maxim: If nobody is questioning or criticizing your security, you have bad security.

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.

Narcissist Maxim: Security managers, bureaucrats, manufacturers, vendors, and end-users will automatically assume that, if they cannot readily conceive of a way to defeat a security product (or a security program), then nobody else can. Remarkably, this will be true even for people with little or no experience, resources, or aptitude for defeating security, and even if they are spectacularly unimaginative.

You Could've Knocked Me Over with a Feather Maxim 1: Security managers, bureaucrats, 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, bureaucrats, 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, and/or maximize your organization's ability to bounce back (resiliency).

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.

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.

Eeny, Meeny, Miny Maxim: The scapegoat(s) chosen after a serious security incident will tend to be chosen from among these 3 groups: those who had nothing to do with the incident, those who lacked the authority and resources to prevent it, and those whose warnings about the possibility of this or related incidents went unheeded.

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

I Question This Maxim Maxim: Skepticism about security (if not all-out cynicism) is almost always warranted. Moreover, it is a powerful tool for analyzing or evaluating security.

Thinking Outside the Bun Maxim: Any security manager who cannot think of a new place to have lunch oversees a poor security program.

Absence of Evidence As Evidence of Absence Maxim: The fact that any given unimaginative bureaucrat or security manager cannot immediately envision a viable attack scenario will be taken as proof that there are no vulnerabilities.

That's Not My Department Maxim: Any employee who's job primarily entails checking on security compliance will have no interest in (or understanding of) security, will not permit it to interfere with his/her job, and will look at you like you are crazy if you raise any actual security concerns.

Deer in the Headlights (I'm With Stupid) Maxim: Any sufficiently advanced cowardice, fear, arrogance, denial, ignorance, laziness, or bureaucratic intransigence is indistinguishable from stupidity.

Cowboy Maxim: You can lead a jackass to security, but you can't make him think.

Awareness Training: Most security awareness training turns employees against security and/or hypocritically represents the organization as having a good security culture when it does not.

See I (Just Work Here) Maxim 1: (Your security awareness or CI training not withstanding) any given Counter-Intelligence (CI) Officer doesn't want to hear about your CI concerns, and will do nothing about them if they are forced upon him/her.

See I (Just Work Here) Maxim 2: Any bureaucrat sufficiently high up in the Security or Counter-Intelligence Department doesn't get Counter Intelligence (CI).

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. Comment: This is a sure recipe for lousy security. Examples include

RFIDs, GPS, and many so-called nuclear Material Control and Accountability (MC&A) programs.

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 and research has gone into it. Comment: Research-based practice is rare in important security applications. For example, while the security of candy and soda vending machines has been carefully analyzed and researched, the security of nuclear materials has not. Perhaps this is because when we have a very important security application, committees, bureaucrats, power grabbers, business managers, and linear/plodding/unimaginative thinkers take over. Also, there is mental paralysis because the stakes are so high.

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. Comment: Thus, after September 11, airport screeners confiscated passengers' fingernail clippers, apparently under the theory that a hijacker might threaten the pilot with a bad manicure. At the same time, there was no significant screening of the cargo and luggage loaded onto passenger airplanes.

Ass Sets Maxim: Most security programs focus on protecting the wrong assets. Comment: Often the focus is excessively on physical assets, not more important assets such as people, intellectual property, trade secrets, good will, an organization's reputation, customer and vendor privacy, etc.

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, how, and by whom). Plus you might even be ok if you get the threats wrong (which you probably will). But if you focus only on the threats, you're likely to be in trouble. Comment: It's hard to predict the threats accurately, but threats (real or imagined) are great for scaring an organization into action. It's not so hard to find the vulnerabilities if you really want to, but it is usually difficult to get anybody to do anything about them.

Vulnerabilities are the Threat Maxim: Security (and emergency response) typically fails not because the threats were misunderstood, but because the vulnerabilities were not recognized and/or not mitigated.

See No Evil Maxim: Organizations and security managers are more afraid of vulnerabilities than threats, so much so that they will often deny that vulnerabilities can exist, rather than address them.

Gap Maxim: People and organizations that talk about "gaps" in their security (rather than vulnerabilities or attack scenarios) have middling security at best. Comment: At least they are able to acknowledge that vulnerabilities can exist (a good thing) but the gap/no-gap binary mindset is not conducive to good security.

Risky Business Maxim: Many of the activities involved in developing or evaluating security measures will only have a partial or superficial connection to true Risk Management.

Stupid Met Tricks Maxim: Any given security metric is more likely to measure security management, compliance with rules, or performance against one very specific (and improbable) attack scenario than actual security. And it probably drives more undesirable security behaviors and attitudes than good ones.

Mermaid Maxim: The most common excuse for not fixing security vulnerabilities is the belief that they simply can't exist. Comment: Often, the evidence offered that no security vulnerabilities exist is that the security manager who expresses this view can't personally imagine how to defeat the security.

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". Comment: Security in Depth has its uses, but it should not be the knee jerk response to difficult security challenges, nor an excuse to stop thinking and improving security, as it often is.

Hopeless Maxim: The third most common excuse for not fixing security vulnerabilities is that "all security devices, systems, and programs can be defeated". Comment: This maxim is typically expressed by the same person who initially invoked the Mermaid Maxim, when he/she is forced to acknowledge that the vulnerabilities actually exist because they've been demonstrated in his/her face. A common variant of the hopeless maxim is "sure, we could implement that inexpensive countermeasure so that the average person on the street couldn't defeat our security with a bobby pin, but then the bad guys would just come up with another, more sophisticated attack".

Takes One to Know One Maxim: The fourth most common excuse for not fixing security vulnerabilities is that "our adversaries are too stupid and/or unresourceful to figure that out." Comment: Never underestimate your adversaries, or the extent to which people will go to defeat security.

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

Waylayered Security Maxim: Complex layered security will fail stupidly. Comment: See, for example, the 82-year old nun penetrating the Y-12 nuclear facility, or the White House fence jumper.

Gatekeeper ("We'll Only Get Suspicious When Bob Does") Maxim: Organizations and security managers will frequently deploy multiple security measures (perhaps layered), but only put them into play if a particular measure (or layer) indicates there might be a problem—thus largely negating the other measures (or layers). Thus, adversaries often need to spoof or neutralize only one key measure to defeat the overall security. Comment: The 1 security measure (or layer) that is relied upon is usually the easiest to interpret. Examples of this maxim: (1) In some facilities, guards do nothing until an audible alarm sounds. (2) If a cargo tamper-indicating seal appears intake, it may not be carefully inspected or its serial number compared with records—thus ignoring most of its security features.

Redundancy/Orthogonality Maxim: When different security measures are thought of as redundant or "backups", they typically are not. Comment: Redundancy is often mistakenly assumed because the disparate functions of the two security measures aren't carefully thought through.

Tabor's Maxim #1 (Narcissism Maxim): Security is an illusionary ideal created by people who have an overvalued sense of their own self worth. Comment: From Derek Tabor. This maxim is cynical even by our depressing standards—though that doesn't make it wrong.

Tabor's Maxim #2 (Cost Maxim): Security is practically achieved by making the cost of obtaining or damaging an asset higher than the value of the asset itself. Comment: From Derek Tabor. Note that "cost" isn't necessarily measured in terms of dollars.

Buffett's Maxim: You should only use security hardware, software, and strategies you understand. Comment: This is analogous to Warren Buffett's advice on how to invest, but it applies equally well to security. While it's little more than common sense, this advice is routinely ignored by security managers.

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. Comment: So named because if the attack or vulnerability was demonstrated on a Tuesday, it won't be viewed as applicable on Thursday. Our favorite example of this maxim is when we made a video showing how to use GPS spoofing to hijack a truck that uses GPS tracking. In that video, the GPS antenna was shown attached to the side of the truck so that it could be easily seen on the video. After viewing the video, one security manager said it was all very interesting, but not relevant for their operations because their trucks had the antenna on the roof.

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. Comment: The name of this maxim comes from the 1633 Inquisition where Church officials refused to look into Galileo's telescope out of fear of what they might see.

Michener's Maxim: We are never prepared for what we expect. Comment: From a quote by author James Michener (1907-1997). As an example, consider Hurricane Katrina.

Black Ops Maxim: If facility security is the responsibility of the Facility Management or (in government) Operations Department, then security will be given about as much importance and careful analysis as snow removal or taking out the trash.

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. Comment: Because if all you can do is threaten people, rather than developing and motivating good security practices, you will not get good results in the long term.

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. Comment: Thus increasing the cynicism regular (non-security) employees have towards security.

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.

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.

Rigormortis Maxim: The greater the amount of rigor claimed or implied for a given security analysis, vulnerability assessment, risk management exercise, or security design, the less careful, clever, critical, imaginative, and realistic thought has gone into it.

Catastrophic Maxim: Most organizations mistakenly think about and prepare for rare, catastrophic attacks (if they do so at all) in the same way as for minor security incidents.

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. Comment: Named for the catch-phrase from the 1960 Stanley Kubrick film *Spartacus*. When the Romans captured Spartacus' army, they demanded he identify himself, but all his soldiers claimed to be Spartacus. Not historically accurate, but very Hollywood!

Band-Aid Maxim: Effective security is difficult enough when designed in from scratch. It can rarely be added on at the end, or as an afterthought. Comment: So plan security at the earliest design stages of a security device, system, or program.

Methodist Maxim: While vulnerabilities determine the methods of attack, most vulnerability or risk assessments will act as if the reverse were true.

Tucker's Maxim #1 (Early Bird & Worm Maxim): An adversary is most vulnerable to detection and disruption just prior to an attack. Comment: So seize the initiative in the adversary's planning stages. From Craig Tucker.

Tucker's Maxim #2 (Toss the Dice Maxim): When the bullets start flying, it's a crapshoot and nobody can be sure how it'll turn out. Comment: So don't let it get to that point. From Craig Tucker.

Tucker's Maxim #3 (Failure = Success Maxim): If you're not failing when you're training or testing your security, you're not learning anything. Comment: From Craig Tucker.

Gunslingers' Maxim: Any government security program will mistakenly focus more on dealing with force-on-force attacks and brute force methods than on more likely attacks involving insider threats and subtle, surreptitious approaches.

We Built This Door for You: The security of most facilities will be based on the wrong idea that the bad guys will use the existing doors, stairs, and hallways to execute an attack. Comment: And security sensors, video cameras, and guards will be dangerously misplaced as a result.

Fool-On-Fool Maxim: The incompetence of any security program is proportional to the degree of obsession with idea that the major threat is a small band of stupid, unprepared adversaries who mindlessly attack straight on, using force and zero insiders. Comment: Somehow, the number of envisioned attackers is always less than the number the security program can purportedly neutralize.

3D Maxim: The incompetence of any security program is proportional to how strongly the mantra of "Deter, Detect, Delay" is embraced. Comment: This philosophy, while theoretically having some merit, is (as a practical matter) strongly correlated with unimaginative, non-proactive security.

D(OU)BT Maxim: If you think Design Basis Threat (DBT) is something to test your security against, then you don't understand DBT and you don't understand your security application. Comment: If done properly—which it often is not—DBT is for purposes of

allocating security resources based on probabilistic analyses, not judging security effectiveness. Moreover, if the threat probabilities in the DBT analysis are all essentially 1, the analysis is deeply flawed.

It's Too Quiet Maxim: "Bad guys attack, and good guys react" is not a viable security strategy. Comment: It is necessary to be both proactive in defense, and to preemptively undermine the bad guys in offense.

Nietzsche's Maxim: It's not winning if the good guys have to adopt the unenlightened, illegal, or morally reprehensible tactics of the bad guys. Comment: "Whoever fights monsters should see to it that in the process he does not become a monster." Friedrich Nietzsche (1844-1900), *Beyond Good and Evil.*

Patton's Maxim: When everybody is thinking alike about security, then nobody is thinking. Comment: Adapted from a broader maxim by General George S. Patton (1885-1945).

Kafka's Maxim: The people who write security rules and regulations don't understand (1) what they are doing, or (2) how their policies drive actual security behaviors and misbehaviors.

30% Maxim: In any large organization, at least 30% of the security rules, policies, and procedures are pointless, absurd, ineffective, naïve, out of date, wasteful, distracting, or one-size-fits-all nonsense, or they may even actively undermine security (by creating cynicism about security, ignoring local conditions, or driving bad behaviors that were not anticipated).

The Politics Maxim: All security is local. Comment: Security depends on the local, on-the-ground conditions, not on high-level idealized plans for security.

By the Book Maxim: Full compliance with security rules and regulations is not compatible with optimal security. Comment: Because security rules and regulations are typically dumb and unrealistic (at least partially). Moreover, they often lead to over-confidence, waste time and resources, create unhelpful distractions, engender cynicism about security, and encourage employees to find workarounds to get their job done—thus making security an "us vs. them" game.

Pink Teaming Maxim: Most so-called "vulnerability assessments" are actually threat assessments, compliance auditing, "Red Teaming", penetration testing, or some other exercise (like security surveys, safety analysis, feature analysis, design basis threat, or performance/reliability testing) not well designed to uncover a wide range of security vulnerabilities. Comment: This is much more the case in physical security than in cyber security. Originally, "Red Teaming" meant doing a vulnerability assessment, but it recent years, it has come to mean a one-off, often rigged "test" of a particular attack scenario. This may have some value, but is not the same thing as a comprehensive vulnerability

assessment looking at a wide range of vulnerabilities. (For compliance auditing, it is important to remember the 30% Maxim. See above.)

It's About More Than Semantics Maxim: Organizations and security managers that misuse (or don't use at all) the terms "vulnerabilities" or "vulnerability assessments" don't do vulnerability assessments. Comment: While semantics aren't very interesting, language does affect thinking.

Aw Ditz Maxim: Mindlessly auditing if bureaucratic security rules are being followed will usually get confused with a meaningful security review, or a vulnerability assessment. Comment: Compliance-based security doesn't really work. See the 30% Maxim above.

Seeing Red Maxim: "Red Teaming" or penetration testing will usually get confused with a comprehensive security review, or a vulnerability assessment.

Rig the Rig Maxim: Any supposedly "realistic" test of security is rigged.

Cyborg Maxim: Organizations and managers who automatically think "cyber", "IT". or "computer" when somebody says "security", don't have good security (including good cyber or computer security).

Caffeine Maxim: On a day-to-day basis, security is mostly about paying attention.

Any Donuts Left? Maxim: But paying attention is very difficult.

Wolfe's Maxim: If you don't find it often, you often don't find it. Comment: Perceptual blindness is a huge problem for security officers.

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. Comment: From *Harry Potter*.

Mahbubani's Maxim: Organizations and security managers who cannot envision security failures, will not be able to avoid them. Comment: Named for scholar and diplomat Kishore Mahbubani. He meant to apply this general principle to politics, diplomacy, and public policy, but it is also applicable to security.

Hats & Sunglasses Off in the Bank Maxim: Security rules that only the good guys follow are probably Security Theater.

Merton's Maxim: The bad guys don't obey our security policies. Comment: This maxim is courtesy of Kevin Sweere. It is named after Thomas Merton (1915-1968), a theological writer and philosopher.

Sweere's Maxim (Merton's Corollary): It's worse than that. The bad guys will analyze our security policies and regulations to find exploitable vulnerabilities, including those not envisioned by the good guys.

Wall Street Maxim: Every good idea is eventually a bad idea.

Dumbestic Safeguards Maxim: Domestic Nuclear Safeguards will inevitably get confused with International Nuclear Safeguards (treaty monitoring), including by people and organizations claiming to fully appreciate that the two applications are very different. Comment: Domestic Nuclear Safeguards is a typical security application, just for very important assets. With International Nuclear Safeguards, in contrast, the bad guys own the assets and facilities of interest, and they fully understand the surveillance, monitoring, and safeguards equipment being used (and may even build, control, and/or install it). It is especially common to overlook or ignore the fact that the adversary in International Nuclear Safeguards is a country, with national- to world-class resources available to defeat the safeguards. [Note: It's sometimes misleading called "International Nuclear Safeguards" when one country or organization, or group of countries try to help a nation improve its own domestic nuclear safeguards, but this is still just Domestic Nuclear Safeguards for the country of interest.]

Werther's Maxim: The security of encrypted (or digitally authenticated) information has less to do with the sophistication of the cipher than with the competence, intelligence, diligence, and loyalty of the people who handle it. Comment: From a quote by Waldemar Werther that "The security of a cipher lies less with the cleverness of the inventor than with the stupidity of the men who are using it."

Tobias's Maxim #5: Encryption is largely irrelevant. Comment: From Marc Weber Tobias.

Red Herring Maxim: At some point in any challenging security application, somebody (or nearly everybody) will propose or deploy more or less pointless encryption, hashes, or data authentication along with the often incorrect and largely irrelevant statement that "the cipher [or hash or authentication algorithm] cannot be broken".

Comment: For many security applications, people forget that "it's no more difficult to copy *encrypted* data than it is to copy *unencrypted* data."

Product anti-counterfeiting tags and International Nuclear Safeguards are two security applications highly susceptible to fuzzy thinking about encryption and data authentication.

With anti-counterfeiting tags, it is no harder for the product counterfeiters to make copies of encrypted data than it is to make copies of unencrypted data. They don't have to understand the encryption scheme or the encrypted data to copy it, so that the degree of difficulty in breaking the encryption (usually overstated) is irrelevant. Indeed, if there was a technology that could preventing cloning of encrypted data (or hashes or digital authentication), then that same technology could be used to prevent cloning of the unencrypted original data, in which case the encryption has no significant role to play. (Sometimes one might wish to send secure information to counterfeit hunters in the field,

but the security features and encryption typically employed on cell phones or computers is good enough.)

What makes no sense is putting encrypted data on a product, with or without it including encrypted data about an attached anti-counterfeiting tag; the bad guys can easily clone the encrypted data without having to understand it. When there is an anti-counterfeiting tag on a product, only the degree of difficulty of cloning it is relevant, not the encryption scheme. The use of unique, one-of-a-kind tags (i.e., complexity tags) does not alter the relative unimportance of the encryption as an anti-counterfeiting measure.

Sometimes people promoting encryption for product anti-counterfeiting vaguely have in mind an overly complicated (and usually incomplete/flawed) form of a virtual numeric token ("call-back strategy"). ([See RG Johnston, "An Anti-Counterfeiting Strategy Using Numeric Tokens", *International Journal of Pharmaceutical Medicine* **19**, 163-171 (2005).]

Encryption is also often thought of as a silver bullet for International Nuclear Safeguards, partially for reasons given in the Dumbestic Safeguards Maxim. The fact is that encryption or data authentication is of little security value if the adversary can easily break into the equipment holding the secret key without detection (as is usually the case), if there is a serious insider threat that puts the secret encryption key at risk (which is pretty much always the case), and/or if the surveillance or monitoring equipment containing the secret key is designed, controlled, inspected, maintained, stored, observed, or operated by the adversary (as is typically the case in International Nuclear Safeguards).

Anti-Silver Bullet Maxim: If you have poor security before you deploy encryption or data authentication, you will have poor security after.
Comment: Sometimes, you'll have worse security because the encryption/authentication provides a false sense of security, or causes distractions.

It's Standard Maxim: As a general rule of thumb, about two-thirds of security "standards" or "certifications" (though not "guidelines") make security worse.

Alice Springs Maxim: Organizations will be loathe to factor in local, on-the-ground details in deciding what security resources to assign to a given location or asset. One-size-fits-all will be greatly preferred because it requires less thinking.
Comment: This maxim is named after the standard reassurance given to worried tourists in Australia that "there aren't a lot of shark attacks in Alice Springs".

Follow the Money Maxim: Security attention and resources will usually be doled out in proportion to the absolute dollar value of the assets being protected, not (as it should be) in proportion to the risk.

Oh, the Lovely Colors! Maxim: High-level corporate executives will be convinced the organization has good security if they are shown lots of detailed, colorful graphs, spreadsheets, and calendars concerning security policies, planning, documentation, and training.

The MBA Maxim: At high levels in an organization, lots of detailed work on security policies, planning, documentation, scheduling, and charts/graphs/spreadsheets will be

preferred over actually thinking carefully and critically about security, or asking critical questions.

Fallacy of Precision Maxim 1: If security managers or bureaucrats assign a number or a ranking to some aspect of security (e.g., probability of attack, economic consequences of the loss of an asset, etc.) they will incorrectly think they really understand that aspect and the related security issues.

Fallacy of Precision Maxim 2: If there are n bits in the attribute measurement of a given object, then security end users can be easily (wrongly) convinced that 2^{-n} is: (1) the probability that a similar object matches this one, and/or (2) the probability that somebody can fool the attribute reader, including by "counterfeiting" or mimicking the object so that it has essentially the same attribute measurement. Comment: End users of security products (especially biometrics or tag readers) will often be fooled by this fallacy. Why is it a fallacy? Among other reasons: Because the bits are not uncorrelated, because they don't all have relevance to the security or authenticity problem (maybe none of them do!), because the degree of correlation between similar objects has not been inputted into the problem, because the type 1 and type 2 errors and tradeoffs haven't been carefully measured or analyzed, because the ease or difficulty of counterfeiting involves many outside factors not included here, and because the ease or difficulty of otherwise spoofing the reader has not been considered.

Apples and Oranges Maxim: Anyone trying to sell you a counterfeit detector, will make a big show of how different objects have different signatures (attribute measurements), but will ignore, oversimplify, or misrepresent the far more important question of how hard it is to fool the reader, including by "counterfeiting" or mimicking the object so that it has essentially the same signature. Comment: Manufacturers, vendors, and promoters of biometrics products and tag readers are very fond of doing this.

I Second That Motion Maxim: "Security by Committee" is an oxymoron.

Nuke that Idea Maxim: Nuclear Security/Safeguards is an oxymoron.

Security By Design Maxim: Most security products, facilities, or programs that were designed using so-called "security by design" methods don't actually have much security in them, but at least the word "security" came up early in discussions.

Lunkhead Maxim: Lunkheads will be attracted to security management and security supervisory roles, including because their ignorance and incompetence will only be occasionally noted.

Executive Protection / Peter Principle / Power Corrupts Maxim: Money spent on protecting high-level executives is wasted, as the organization would be much better off without the arrogant, narcissistic, misogynistic morons.

The following are general "laws" that also apply to security:

Fudd's Law: If you push on something hard enough, it will fall over.

First Law of Revision: Information necessitating a change of design will be conveyed to the designers after—and only after—the plans are complete.

Hellrung's Law: If you wait long enough, it will go away.

Grelb's Law: But if it was bad, it will come back.

Brien's First Law: At some time in the life cycle of virtually every organization, its ability to succeed in spite of itself runs out.

Bucy's Law: Nothing is ever accomplished by a reasonable person.

Stewart's Law: It is easier to get forgiveness than permission.

Horngren's Law: The Real World is a special case.

Glazer's Law: If it's "one size fits all", then it doesn't fit anybody.

Gold's Law: If the shoe fits, it's ugly.

Firestone's Law: Chicken Little only has to be right once.

Shaw's Law: Build a system that even a fool can use, and only a fool will want to use it.

Byrne's Law: In any electrical circuit, appliances and wiring will burn out to protect the fuses.

Ginsberg's Laws from the beat poet Allen Ginsberg (1926-1997):
The First Law of Thermodynamics: "You can't win."
The Second Law of Thermodynamics: "You can't break even."
The Third Law of Thermodynamics: "You can't quit."

Putt's Law: Technology is dominated by two types of people: those who understand what they do not manage, and those who manage what they do not understand.

Clarke's First Law: When a distinguished but elderly scientist states that something is possible, he is almost certainly right. When he states that something is impossible, he is probably wrong.

Hawkin's Law: Progress does not consist of replacing a theory that is wrong with one that is right. It consists of replacing a theory that is wrong with one that is more subtly wrong.

Schryver's Law: Sufficiently advanced incompetence is indistinguishable from malice.

Dunning-Kruger Effect: Incompetent people don't recognize that they are incompetent.

Sallinger's Law: All morons hate it when you call them a moron. Comment: From J.D. Sallinger (1919-2010).

Kernighan's Law: Debugging is twice as hard as writing the software in the first place. Therefore, if you write the software as cleverly as possible, you are (by definition) not smart enough to debug it.

Life Cycle of a Good Idea Law: If you have a good idea: first they ignore you, then they ridicule you, then they claim to have thought of it first, then it's declared to be obvious.

Not Invented Here Law: If it wasn't invented here, it's a bad idea (unless we can steal the idea and make it look like we thought of it first).

Glass Houses Law: The people most obsessed with the work quality of others will typically be among the most incompetent, deadwood screw-ups in the whole organization.

Tacitus's Law: To show resentment at a reproach is to acknowledge that one may have deserved it. Comment: From Tacitus (55-117 AD).