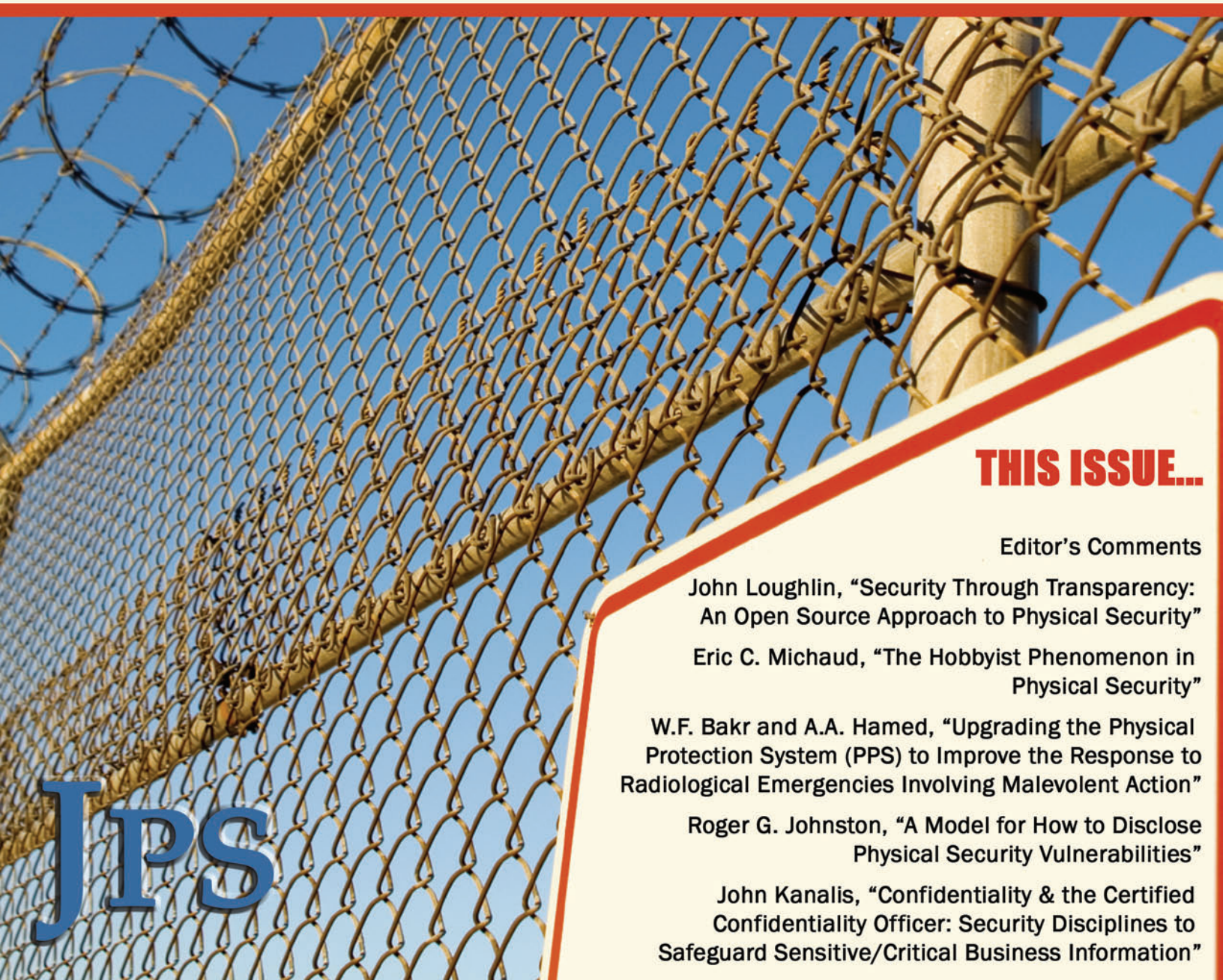
Argonne NATIONAL LABORATORY

The Journal of Physical Security

Volume 3(1), 2009



JPS

THIS ISSUE...

Journal of Physical Security, Volume 3

Table of Contents

Editor's Comments

This is the first issue of *The Journal of Physical Security* (JPS) hosted by Argonne National Laboratory. We'd like to thank Argonne for their support.

JPS will continue to be a scholarly, peer-reviewed, multidisciplinary journal devoted to physical security research, development, modeling, and analysis. Papers from both the technical and social sciences are welcome.

As always, the views expressed by the editor and authors in JPS are their own and should not necessarily be ascribed to Argonne National Laboratory, the United States Department of Energy, or the United States Government.

This issue contains an eclectic mixture of topics. The first two papers are about the emerging issue of Open Sourcing for physical security. Open Sourcing has long been a common practice for software, but is relatively rare for security hardware. The remaining papers discuss a design basis threat approach to protecting a radiological source in a hospital, when and how to disclose physical security vulnerabilities, and a discussion about business confidentiality and protecting sensitive information.

In the last issue, I offered some fairly cynical Security Maxims that were intended to be only partially tongue-in-cheek. These were general rules of thumb that I believe apply about 90% of the time to physical security programs and applications. They have proven to be wildly popular based on the feedback I have received from several hundred people. Curiously, most of these people work in cyber security, not physical security. I'm not sure what that says about the two communities, or the two fields.

At any rate, I present below an updated list of maxims based on additional thinking about these issues, as well as suggestions and input from other security professionals. The newest ones are in red.

Whether you agree with any, all, or none of these, I hope they provide food for thought.

Thank you for reading our journal, and please consider submitting a manuscript, and encouraging your security colleagues to do so as well.

--Roger Johnston, Argonne National Laboratory, June 2009

Security Maxims

While these security maxims are not theorems or absolute truth, they are typically valid ~90% of the time for physical security, and may have applicability to cyber security as well.

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: This is probably 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.

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".

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.

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 problem, whereas the bad guys typically attack deliberately and intelligently, not randomly. For a discussion of the reverse problem, 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.

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

Comment: Tom Baker as Dr. 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.

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

Schneier's Maxim #2 (Control Freaks Maxim): Control will usually get confused with Security.

Comment: 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".

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.

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.

Colsch's (Keep It Simple) 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.

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

Comment: This is one of the reasons why open source security 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.

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

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 as the adversary, not people, and instinctively think about systems failing stochastically, rather than due to deliberate, intelligent, malicious intent.

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.

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 & 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.

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 is a wide range of well-established tools for mitigating disgruntlement. Most are quite inexpensive.

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).

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.

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.

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.

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

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.

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 intangible assets such as 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 all wrong. But if you focus only on the threats, you're probably 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.

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".

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.

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."

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, and intelligent thinking that has been undertaken is inversely proportional to how strongly the strategy of "Security in Depth" (layered security) is embraced.

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: 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: 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.

Comments: 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.

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.

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

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

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.

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.

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.

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

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*. There are important lessons here for homeland security.

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.

By the Book Maxim: Full compliance with security rules and regulations is not compatible with optimal security.

Comment: Because security rules & 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.

Cyborg Maxim: Organizations and managers who automatically think "cyber" 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.

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.

Mahbubani's Maxim: Organizations and security managers who cannot envision security failures, will not be able to avoid them.

Security Through Transparency:

An Open Source Approach to Physical Security

John P. Loughlin
Stanton Concepts
Lebanon, NJ
jpl@stantonconcepts.us

"Security through obscurity" has never been a sensible approach and now—with the Internet—is no longer achievable. A Google query on "lock picking" generates about 4,500,000 returns. There are about 10,000 videos on YouTube related to lock picking. Many bypass methods have gained wide attention including bumping and shimming as well as more sophisticated attacks on "high security" locks. Additionally, lock picking has become a popular sport. For example; www.locksport.com has 14 chapters in the US and Canada; Lockpicking 101 (www.lockpicking101.com) is a club with 60,000 members and its site has a forum to discuss and collaborate on picking and bypass techniques; The Open Organization Of Lock pickers (TOOOL) is based in The Netherlands and is the host and sponsor the annual Dutch Open lock picking competition. NDE (Non Destructive Entry) (www.ndemag.com) is an on line periodical that caters to the lock sport community. The lock sport community is composed predominantly of "white hats" that can play a vital role in the improvement of security hardware.

The general historic nature of the security hardware industry is to have their technology closed to the outside world. They are extremely averse to the hacking of their products and any revelation of vulnerabilities, real or perceived. The reasons for their position might include an obsolete mindset, a very large installed base of potentially vulnerable hardware, fear of tarnishing the brand name, and a diminished reputation for security products. In most cases, they can only delay, not prevent the inevitable; what is not revealed in the patents can be discovered by reverse engineering and will eventually be made public. The products that make the boldest claims tend to be the most inviting targets.

Even if a lock manufacturer discovered a vulnerability and chose to disclose the information; most deployed locks cannot be upgraded easily or in a cost-effective manner.

Stanton Concepts (SCI) has developed a new lock technology along with a new philosophic approach: the design information is open to the outside world.

Our lock cylinder employs well-known, time-tested, rotary mechanical lock mechanisms, while designing out many of the traditional vulnerability issues including bumping, picking, key control and key impressioning. There is no keyway to allow exploitation, observation, or manipulation of individual components. The key is designed with a novel means to manipulate the cylinder and provide management, control, and authorization features including audit trail (who, when, where etc.). The key is intended to change and improve as technology evolves. The resulting Robotic Key System (RKS) is a marriage of established mechanical elements with the new and ever changing state of electronic art.

To achieve these objectives, SCI decided that certain elements of the lock system should be Open Source. Open Sourcing has become increasingly common in software including IT security applications. Some of the more prominent Open Source software products include the Linux operating system, the Apache web server, and the Firefox web browser. The Open Source Software Initiative (OSI) is a non-profit organization that is actively involved in the Open Source community; their goal is to build and educate the community and meet with the public and private sectors to promote and discuss how Open Source Software technologies, licenses and development approaches can provide economic and strategic advantages.

OSI summarizes Open Source Software (OSS) on their website as:

"Open Source is a development method for software that harnesses the power of distributed peer review and transparency of process. The promise of open source is better quality, higher reliability, more flexibility, lower cost, and an end to predatory vendor lock-in."

OSI further defines Open Source Software as software that include these primary attributes; free distribution, inclusion of source code, no discrimination against persons or groups and no discrimination against fields of endeavor. Their definition also addresses licensing.

Open Source Hardware (OSH) is also becoming popular, including hardware for gaming, computer components, robotics, and telephony, but does not exist for security hardware. The term Open Source Hardware (OSH) primarily relates to hardware that is electronic in nature and implies the free release of the design information including schematics, bills of material, and PCB layout data. Open Source Software (OSS) is often used to drive the Open Source Hardware.

Predating both the Open Source software and hardware movements is an Open Source approach to cryptography which has been applied for years with great success. According to Bruce Schneier, (www.schneier.com), a leading expert in cryptography and computer security: "In the cryptography world, we consider Open Source necessary for good security; we have for decades. Public security is always more secure than proprietary security. It's true for cryptographic algorithms, security protocols, and security source code. For us, Open Source isn't just a business model; it's smart engineering practice."

The essential difference between software and hardware is that the hardware is a physical object that costs money to develop, prototype, manufacture and distribute. Software licenses rely on copyright law while hardware licenses rely on patent law.

The RKS has two primary elements; a mechanical lock cylinder and an electro-mechanical key. The key or Robotic Dialer includes electronic hardware and software. The cylinder is in the low-tech domain and the dialer is in the high tech domain.

The low-tech cylinder (figure 1) is a simple, stable, proven, and reliable lock mechanism that is highly resistant to manipulation. In addition, it has low cost and is environmentally robust. To quote Leonardo Da Vinci; "Simplicity is the ultimate sophistication". The cylinder can be a drop-in replacement for existing "high security" key cylinders; its form factor can be smaller or larger depending on the application.

Figure 1 - The low-tech locking cylinder

The cylinder is a purely mechanical device that uses a combination type of lock mechanism. It has, however, a greater number of combinations ("keyspace") compared to conventional high security, manually operated combination locks. There is no keyway, and the lock cannot be finger-manipulated. The mechanical design yields several billion possible combinations. The assembly consists only of approximately 10 unique parts, with a total of about 30 parts overall, and is highly manufacturable. The RKS cylinder is currently commercially available in limited quantities.

A cylinder with 6 discs, each disc having 36 variations, theoretically yields 36^6 = 2,176,782,336 possible combinations. A 6-disc lock requires > 21 combined clockwise and counter-clockwise revolutions for alignment. The dialer in Figure 2 can dial a combination in about 3.5 seconds at an average RPM of 360. However, engineering may reduce the dialing to ~2 seconds. For example, if we reduce the number of combinations from $2.2X10^9$ to $1X10^9$, and assume 2 seconds per combination, it would take an adversary 6 years of brute-force sequential dialing to cycle through the entire keyspace. The mass and momentum of the lock mechanism also limits the speed of an attack.

The RKS Dialer used in conjunction with the cylinder is a portable electro-mechanical device that engages the cylinder. See figure 2. Once the Dialer user is authorized via a password or personal identification number (PIN), the dialer looks up the opening code in an onboard or remote database,

and then opens the lock by driving the cylinder's discs in the proper clockwise and counter-clockwise sequence.

Figure 2 - The RKS Dialer than unlocks the cylinder shown in figure 1.

Because the possible additional features and functions for the dialer are virtually limitless (GPS, biometrics, encryption, RFID, cellular and wireless etc.), the strategy is to provide a basic platform that includes an inexpensive and widely used PIC microcontroller (Microchip PIC16F917), motor controller, clock, EPROM, and a DC servomotor. The basic dialer can store a multitude of lock combinations. It uses PIN-based access control, has programmable time-out periods for specific locks and operators, and keeps a record of all activity. The dialer also has a USB interface to facilitate communication with a PC or Mac. This basic platform may be used for real world physical security applications, or as a development platform.

The Robotic Dialer is a natural for Open Source development. While the lock cylinders may be part of an installed base (perhaps located in uncontrolled environments), the dialer is portable and free to evolve independently and in real time. There is really no limit to the technology the Robotic Dialer could employ. The motor and dialing components could also be a subassembly designed to mate with an iPhone or other hand held computing device. Some or all of the management and control software could reside on the hand held device.

Currently, there are a number of advanced smart locks in the market place that involve a smart key that engages mechanically and electronically with a smart cylinder. These devices all use proprietary encryption schemes. Keeping the smart cylinders up-to-date with the latest software can be challenge when the locks are deployed over a large area. Another concern is that once a crack or bypass is uncovered—either by reverse engineering, intellectual persistence, or application of new and sophisticated tools—the information can be distributed at quickly, and every deployed lock will then be compromised.

Different users could develop Open Source hardware, software and encryption algorithms for the RKS dialer to meet their own specific needs and agendas. There could also be a collaborative effort among interested parties. Because the dialer is detached technologically from the cylinder, one party's dialer

would not have or (be able to) derive the opening information for another party's lock. The lock remains secure simply because of the extremely large number of possible permutations and the cylinder's intrinsic pick resistance. Also, unlike master key systems, disassembling one RKS lock cylinder reveals nothing about how the other RKS locks are combinated. As discussed above, determining the combination by sequential dialing is impractical because of the time required.

Of course there are pros and cons to Open Sourcing. The positive aspects include free software, transparent and available source code, community support, the fact that anyone can participate, security through many eyes, and the leveraging of a huge knowledge base. For security products, the only way to achieve a high degree of confidence is to have them examined by many experts. Another important positive aspect is that Open Sourcing gives companies that lack an Open Source approach an incentive to try harder to improve the security of their products.

Some of the negative aspects include licensing and IP issues, a complicated revenue model, lack of central control, issues associated with having many different versions of the same applications, documentation and support problems, and the fact that nefarious hackers have access as well as the end users.

There are several licensing models for both Open Source hardware and software products. In the case of the RKS, for example, Stanton Concepts could retain rights to the lock cylinder and mechanical interface. The lock cylinder would then be purchased or licensed, the dialer could also be purchased but the schematic, firmware, bill of material, and PCB data would be available under a Group Public License (GPL). The control software would also be Open Source, enabling users or organizations to develop and distribute software to suit their needs. Distinctions could also be made for commercial and non-commercial use.

In the view of Stanton concepts, the positive aspects of the Open Source approach far outweigh the negative. Open Sourcing allows interested parties to collaborate, continually improve, and expand the functionality and security of the lock system. The product is not constrained by one company's limited ability and/or closed architecture. The design would be more agile and vulnerabilities would be identified and hopefully addressed quickly and in a transparent manner.

Stanton Concepts agrees with Bruce Schneier in that not only is an Open Source approach a good business model, but it is also a smart engineering practice. The RKS is new and its future is uncertain, but we feel strongly that its unique design along with an Open Source approach bode well for its success.

Journal of Physical Security 3(1), 6-8 (2009).

Viewpoint Paper

The Hobbyist Phenomenon in Physical Security*

Eric C. Michaud
Vulnerability Assessment Team
Argonne National Laboratory
emichaud@anl.gov

Pro-Ams (professional amateurs) are groups of people who work on a problem as amateurs or unpaid persons in a given field at professional levels of competence. Astronomy is a good example of Pro-Am activity. At Galaxy Zoo [1], Pro-Ams evaluate data generated by professional observatories and are able to evaluate the millions of galaxies that have been observed but not classified, and report their findings at professional levels for fun. To allow the archiving of millions of galaxies that have been observed but not classified, the website has been engineered so that the public can view and classify galaxies even if they are not professional astronomers. In this endeavor, it has been found that amateurs can easily outperform automated vision systems.

Today in the world of physical security, Pro-Ams are playing an ever-increasing role. Traditionally, locksmiths, corporations, and government organizations have been largely responsible for developing standards, uncovering vulnerabilities, and devising best security practices. Increasingly, however, non-profit sporting organizations and clubs are doing this. They can be found all over the world, from Europe to the US and now South East Asia. Examples include TOOOL (The Open Organization of Lockpickers), the Longhorn Lockpicking Club, Sportsfreunde der Sperrtechnik – Deustcheland e.V., though there are many others. Members of these groups have been getting together weekly to discuss many elements of security, with some groups specializing in specific areas of security. When members are asked why they participate in these hobbyist groups, they usually reply (with gusto) that they do it for fun, and that they view defeating locks and other security devices as an interesting and entertaining puzzle.

A lot of what happens at these clubs would not be possible if it weren't for "Super Abundance", the ability to easily acquire (at little or no cost) the products, security tools, technologies, and intellectual resources traditionally limited to corporations, government organizations, or wealthy individuals. With this new access comes new discoveries. For example, hobbyist sport lockpicking groups discovered—and publicized—a number of new vulnerabilities between 2004 and 2009 that resulted in the majority of high-security lock manufacturers having to make changes and improvements to their products. A decade ago, amateur physical security discoveries were rare, at least those discussed publicly. In the interim, Internet sites such as lockpicking.org, lockpicking101.com and others have provided an online meeting place for people to trade tips, find friends with similar interests, and develop tools.

*Editor's Note: This paper was not peer reviewed.

The open, public discussion of software vulnerabilities, in contrast, has been going on for a long time. These two industries, physical security and software, have very different upgrade mechanisms. With software, a patch can typically be deployed quickly to fix a serious vulnerability, whereas a hardware fix for a physical security device or system can take upwards of months to implement in the field, especially if (as is often the case) hardware integrators are involved.

Even when responding to publicly announced security vulnerabilities, manufacturers of physical security devices such as locks, intrusion detectors, or access control devices rarely view hobbyists as a positive resource. This is most unfortunate.

In the field of software, it is common to speak of Open Source versus Closed Source. An Open Source software company may choose to distribute their software with a particular license, and give it away openly, with full details and all the lines of source code made available. Linux is a very popular example of this. A Close Source company, in contrast, chooses not to reveal its source code and will license its software products in a restrictive manor. Slowly, the idea of Open Source is now coming to the world of physical security. In the case of locks, it provides an alternative to the traditional Closed Source world of locksmiths.

Now locks are physical objects, and can therefore be disassembled. As such, they have always been Open Source in a limited sense. Secrecy, in fact, is very difficult to maintain for a lock that is widely distributed. Having direct access to the lock design provides the hobbyist with a very open environment for finding security flaws, even if the lock manufacturer attempts to follow a Close Source model.

It is clear that the field of physical security is going the digital route with companies such as Medeco, Mul-T-Lock, and Abloy manufacturing electromechanical locks. Various companies have already begun to add microcontrollers, cryptographic chip sets, solid-state sensors, and a number of other high-tech improvements to their product lineup in an effort to thwart people from defeating their security products. In my view, this as a somewhat dangerous development because many physical security companies are not holding themselves to the same standards and sophistication as companies in, for example, the software or casino industries. It is irresponsible, in my view, for a manufacturer or vendor to label a product is “secure” solely because there are billions of possible digital combinations, particularly when there are examples of software being used by an adversary to try all possible combinations.[2]

I would like to see manufacturers of physical security products and Pro-Ams groups come to some agreed upon mechanism for the latter to disclose security vulnerabilities to the former. Essential in any such mechanism is the need to avoid shooting the messenger, threatening researchers or hobbyists, or suing anybody when vulnerabilities are discovered. It is essential for manufacturers to take the vulnerabilities seriously, and fix the issues that can be readily mitigated. Manufacturers and Pro-Ams should not be at odds with each other, but should instead work together to improve security.

Considering that there is surprisingly little extensive research and development in the physical security field, even less imaginative testing, and a lack of effective vulnerability assessments for physical security products, the industry leaders need to take a proactive step forward. Manufacturers need to stop ignoring security experts (Pro-Ams or otherwise) when designing new products and

evaluating current ones. Critical, knowledgeable input is especially important when physical security products are in their infancy, and crucial changes can be easily implemented. Effective use of Pro-Ams will prove to be essential in the upcoming years as cutting edge technologies continue to be implemented in new security products while also becoming more and more accessible to the general public. Indeed, a good first step can be seen in the open letter Peter Fields of Medeco wrote to the locksport community magazine Non-Destructive Entry.[3]

References

1. "Galazy Zoo", http://en.wikipedia.org/wiki/Galaxy_Zoo

2. Richard Clayton, "Brute Force Attacks on Cryptographic Keys", http://www.cl.cam.ac.uk/users/rnc1/brute.html

3. Peter Field, "An Open Letter to the Sport Lock-Picking Community", Non-Destructive Entry, http://ndemag.com/nde3.html

Upgrading the Physical Protection System (PPS) To Improve the Response to Radiological Emergencies Involving Malevolent Action

W.F.Bakr and A.A.Hamed

Radiological Regulations and Emergency Division
National Center for Nuclear Safety and Radiation Control
EAEA
Cairo, Egypt
email: wafaaf_75@yahoo.com

Abstract

Experience in many parts of the world continues to prove that movements of radioactive material outside of the regulatory and legal framework may occur. The aim of this article is to discuss a proposed physical protection system for improving the protection of radioactive sources used for medical purposes.

Introduction

The threat from criminal activities can include bomb threats, bombings, sabotage, vandalism, physical attacks, kidnapping, hostage-taking, theft of radioactive or fissionable material, or other criminal acts potentially resulting in an actual or perceived radiation emergency. Experience shows that the public's perception of the risk posed by the threat may be more important than the actual risk. Consequently, an important part of a security program is providing the public, ideally in advance of an attack, with timely, informative (understandable) and consistent information on the true risk.[1].

Many factors can lead to loss of control of radioactive sources, including ineffective regulations and regulatory oversight; the lack of management commitment or worker training; poor source design; and poor physical protection of sources during storage or transport. The challenge is to address this wide range of risks with effective actions. [2]. Effective physical protection requires a designed mixture of hardware (security devices), procedures (including the organization of the guards and the performance of their duties) and facility design (including layout) [3]. One of the most important aspects of managing a radiological emergency is the ability to promptly and adequately determine the threat and take appropriate actions to protect members of the public and emergency workers.

Objective

This article is focused on the study of the current status of the physical protection system (PPS) for a radioactive source used in a tele-therapy unit in a public hospital. Hazard assessment is calculated and Design Basis Threat (DBT) is proposed. The process utilizes a performance-based system to design and analyze PPS effectiveness for the protection of the radioactive

source. We also analyze how this design improves the response to radiological emergencies involving malevolent action.

Methodology

The ultimate goal of a Physical Protection System (PPS) is to prevent the accomplishment of overt or covert malevolent actions. Typical objectives are to prevent sabotage of critical equipment, deter theft of assets or information from within the facility, and protect people. A PPS must accomplish its objectives by either deterrence or a combination of detection, delay, and response [4]. In attempting to address the threats from malevolent acts involving radioactive sources, it is clear that radiological sources of certain magnitudes and types are more attractive to those with malevolent intent than others [5]. The present study involves the steps A-F discussed below for the proposed PPS.

A- Asset and Site Assessment:

A ^{60}Co source with an activity of 7494 Ci (277.27 TBq) as of March, 1999 is used by a Tele-therapy Unit in a public hospital for the treatment of patients. The working hours are 9.00 am to 2.00 pm daily. Fig.(1) illustrates the layout of the hospital including the main gates.

The hospital gates are: Gate 1 is for employees and a clinical unit, closed at 2.00 pm; Gate 2 is for patients, open 24 hours. Gates 1&2 are the main gates; Gate 3 is emergency gate, open 24 hours; Gate 4, is for the hospital's receivables; Gate 5 is for external treatment (medical investigation unit), closed at 1.30 pm; and Gate 6 is for the family medical care unit, closed at 6.00 pm.

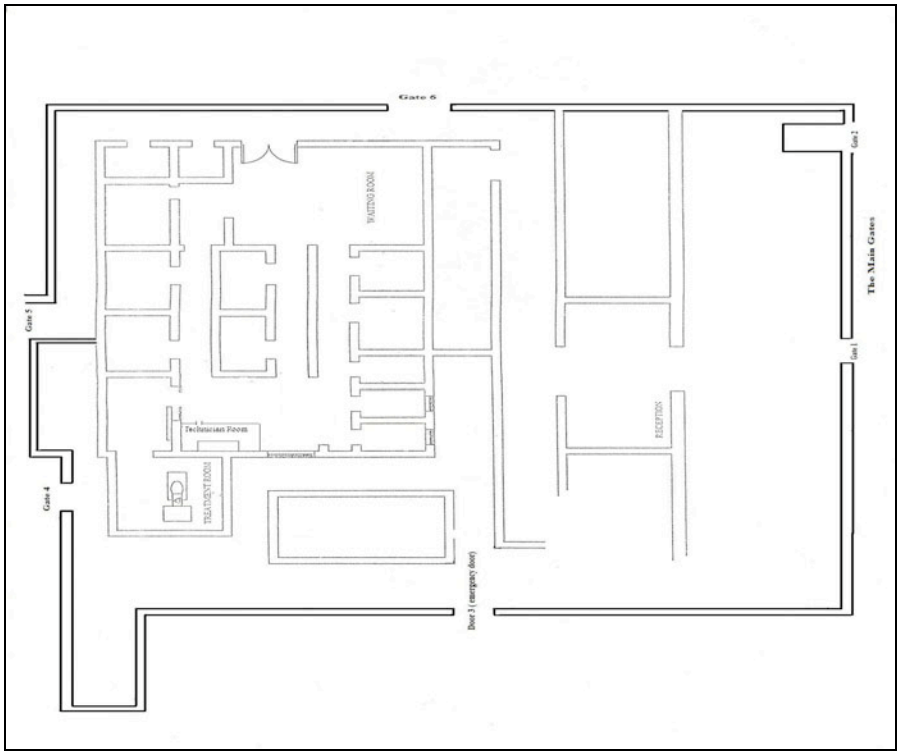


Fig. 1 Lay out of a Public Hospital and the Room for the Tele-therapy Treatment

B- Current Status of the Security System:

A concrete fence of height 2.5 meters defines the external boundaries of the hospital. The room for the tele-therapy unit is covered with windows supported by steel. There is only a monitoring camera in the main hole (waiting area in the first floor); the recorded video is monitored by security personnel. All the entrance gates are opened and connected to each other (you can enter to the hospital's utility from any gate). There is one access to the tele-therapy room, and the door is locked manually. *The functions of PPS in the hospital are thus initially dependent mainly on the initial response of the security guards; in the event of intrusion, they call the police for help, through the police office is located 500 m away from the hospital. Thus, upgrading the PPS is necessary to cover the main three functions (detection, delay, and response) for ensuring the security and safety of the radioactive source.*

C- Risk Assessment and Action Level

The risks are assessed on the assumption that the source or material of interest is not being managed safely or kept securely. A fire or destructive accident could lead to removal of the protecting shield of the radioactive material. The decommissioning of the tele-therapy unit could lead to the same risk if someone would try to remove the radioactive material from the head (protecting shield) of the tele-therapy unit for shipping [1]. Because similar sources worldwide number in the millions, the security measures should be directed at those sources that pose the greatest risks. With this in mind, the IAEA in October of 2003 developed a new categorization system for radioactive sources [6], to ensure that the sources are maintained under a control commensurate with the radiological risks. This categorization system is based on the potential for radioactive sources to cause deterministic effects, i.e., *health effects which do not appear until threshold value is exceeded and for which the severity of effect increases with the dose beyond the threshold*. An amount of radioactive material is considered "dangerous" if it could cause permanent injury or be immediately life threatening if not managed safely and contained securely [1]. The risk factor is calculated through the following equations**:**

For all materials (individual source):

$$D_{f1} = \frac{A}{D} = \sum \frac{A_i}{D_{1,i}} \text{ ---------- (1)}$$

Where D_f is the risk factor, (its value ranges from < 0.01 to > 1000.0).
A_i is the activity (TBq) of each radionuclide over which control could be lost during an emergency/event.
$D_{1,i}$ is constant for isotopes, and is citied in appendix 8 of ref. [1].

For dispersible material:

$$D_{f2} = \frac{A}{D} = \sum \frac{A_i}{D_{1,i}} \text{ ---------- (2)}$$

Where A_i is the activity (TBq) of each radionuclide i that is in a dispersible form over which control could be lost during an emergency/event.
$D_{2,1}$ is constant for isotopes, and is citied in appendix 8 of ref. [1].

Table (1) illustrates the D_{f1} and D_{f2} values of the Co-60 source used in the hospital and the associated risk. From the calculation of A/D value, the source is categorized as category 1 as described in reference [6].

Table (1): The calculated D_{f1} and D_{f2} Values and their associated risk

Activity TBq 277.27	D_{f1} Value 9242.6	D_{f2} Value 9.242
Associated Risk	***Very dangerous to the person:*** This amount of radioactive material, if not managed safely and kept securely, could cause permanent injury of a person who handless it or is otherwise in contact with it for a short time (minutes to hours). It could possibly be fatal to be close to unshielded material for a period of hours to days.	***Dangerous to the person*****:** This amount of radioactive material, if not managed safely and kept securely, could cause permanent injury of a person who handles it or is otherwise in contact with it for some hours. It could possibly — although it is unlikely — be fatal to be close to this amount of unshielded material for a period of days to weeks.

D- Threat Assessment and Design Basis Threat (DBT)

The *Design Basis Threat* for sources must consider the attributes and characteristics of potential insider and/or external adversaries who might attempt to damage or seek unauthorized removal of radioactive sources, against which the PSS is designed and evaluated. The use of a design basis threat assessment methodology is recommended by the IAEA as the best method to design the security measures for specific sources [5]. For our case, the risk involving radioactive source is therefore considered to be quite high. An analysis was performed for the possible consequences of unauthorized acquisition of these radioactive sources from the hospital. This analysis showed that, the nature and form of the ^{60}Co sources are in such that the radioactive material could be easily dispersed via an explosion or otherwise destructive device. On that basis, the specific design basis threat is the possible acquisition of a tele-therapy source by an insider in the hospital or by people who enter the hospital as patients or contractors. Based on the vulnerability analysis for a specific source, an assessment of the risk can be made. The level of this risk will determine the security measures required to protect the source. The higher the risk, the more capability will be required from the security systems [5].

Four security groups are defined based on these fundamental protection capabilities. They provide a systematic way of categorizing the graded performance objectives required to cover the range of security measures that might be needed, depending on the assessed risk. In our case, the security level required was considered to be equivalent to the performance requirements in Security (Group A) in which measures should be established to deter unauthorized access, and to detect unauthorized access and acquisition of the source in a timely manner. These measures should be such as to delay acquisition until response is possible [6].

E- Suggested PPS and Design Criteria

In designing the PPS, we take into consideration a feature-based design and a performance-based design. On the base of the worst case of threat, a proposed PPS was designed. Figs. 2&3 show the suggested access and their locations. This system incorporates the three key functions (detection, delay and response). It also has the capability to verify the various roles of the proposed system: **in-depth protection, balanced protection, and timely detection/response.** The PPS was applied in two protection zones (control room and treatment room) and in the Entrance (door no.2 and the emergency door, as well as the exists of the hospitals).

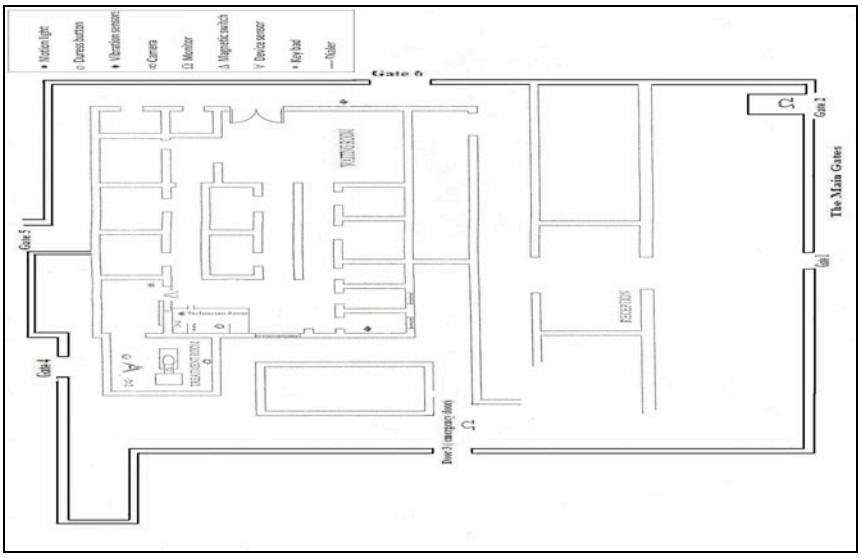


Fig.2 The Suggested Access with their Locations in the Hospital

Fig.3 The Locations of the purposed Equipments in the Tele-therapy Unit

I- Detection Function:

Zone 1: Vibration sensor, Glass break sensor, Duress button, Motion light, Cameras and Dialer.
Zone 2: Balanced magnetic switch (door-device), Microwave sensor, Passive Infra Red (PIR) sensors, Duress button, Sources sensor, Camera and Motion light**.** These functions are attached with *alarm assessment* for all sensors and connected to Video monitors and Sirens in three positions (door 2, door 3" emergency door" and security room). The measures of effectiveness for the detection function are the probability of sensing adversary action, the time required for

reporting and assessing the alarm, and nuisance alarm rate [3]. The proposed system can provide: Timely Detection, Balanced Detection, and Protection in Depth.

II- Delay Function:

The effective source access delay system includes the two elements:

II-1- Physical Barriers

Zone 1: Hardened doors in the 3 entrances, Key control systems for three doors, and Steel on the Windows.

Zone 2: High security hardened door with keypad and lock (password – key) and another hardened door with key.

II-2- Protective Force

■ 2 well -rained Guards are to be present in the Radiotherapy Dept. (Patrolling- closed doors-monitoring).

■ 2 well trained Guards are to be present at Door 2& 3 (Quick response- evaluation of the situation – Quick communication).

■ A police officer is to be present at Door 3 .

The measure of the delay effectiveness is the time required by the adversary (after detection) to bypass each delay element [5].

III- Response:

The response function consists of the actions taken by the response force to prevent adversary success. Response, as it is used here, consists of interruption. Interruption is defined as a sufficient number of response force personnel arriving at the appropriate location to stop the adversary's progress. It includes communicating to the protection force of accurate information about adversary actions and the deployment of the response force. The effectiveness measure of this function is the probability of deployment at the adversary location and the time between receipt of a communication of adversary action and the interruption of the adversary action (response force time RFT) [4].

Development of the response may be established through the following steps:

- Developing of Memorandum of Understanding (MOU) for security and police officers,
- Effective training of security officer,
- Implementation of the authorized security devices to permit fast response,
- Documentation of all procedures.

F- Measuring the Effectiveness of the Proposed PPS

A Computerized EASI Model [4] was used to calculate the probability of interruption (P_I). It is a simple calculation tool that quantitatively illustrates the effect of changing physical protection parameters along a specific path. It uses detection, delay, response, and communication values to compute the probability of interruption P_I. In this model, input parameters representing the physical protection functions of detection, delay, and response are required. Communication likelihood of the alarm signal is also required for the model. Detection and communication inputs are in the form of probabilities (P_D and P_C respectively) that each of these total functions will be performed successfully. Delay and response inputs are in the form of mean times (T_{delay} and RFT respectively) and standard deviations for each element. All inputs

refer to a specific adversary path [4].

Table (2) describes the path of an adversary and the expected P_D values, the delay times, Response Force Time and the calculated P_I.

Table (2): The Calculated Probability of interruption as the function of the PPS Effectiveness

Response Force Time (in Second): 300 sec. Standard deviation: 90			
Probability of Guards communication: 0.95			
Worst path Segments	***P_D***	***Delay Time (Sec.)***	***Standard deviation***
Penetrate site Boundary	0	10	3.0
Cross hospital property	0	10	3.0
Enter Main Door	0	5	1.5
Cross Main Lobby	0	5	1.5
Penetrate Door to Room	0.9	60	18.0
Cross Rad. Treatment Room	0.9	90	27.0
Remove Source & Pack	0.9	360	108
Cross Rad. Treatment Room	0.9	30	9.0
Exit Door to Room	0.7	10	3.0
Exit Emergency Room	0.8	10	3.0
Cross hospital Property	0	5	1.5
Exit Site Boundary	0	5	1.5
Probability of Interruption: 0.9			

Conclusion

The ultimate goal of a Physical Protection System (PPS) is to prevent the accomplishment of overt or covert malevolent actions.

This Study covers the use of a systematic and measurable approach to the design of a PPS. It emphasizes the concept of detection, followed by delay and response.

The proposed performance-based Physical Protection System (PPS) appears to have the capability of defeating adversaries for which it is designed.

Verification of timely detection for intrusion is one of the principles in the proposed system based on use of the included sensors, signal lines, and alarm displays.

The study is considered as base guidelines for the application of PPS in any radioactive facilities.

References

1- EPR-METHOD (2003) Emergency Preparedness and Response Method for Developing Arrangements for Response to a Nuclear or Radiological Emergency Updating IAEA-TECDOC-953.
2- El Baradei, M. (IAEA Director General), Address at the International Conference on Security of Radioactive Sources, Vienna, 11–13 Mar. 2003.
3- IAEA INFCIRCL 225/ rev.4 Corrected, "The Physical Protection of Nuclear Materials and Nuclear Facilities" June 1999.
4- Design and Evaluation of Physical Protection Systems, Mary Lynn Garcia.

5- IAEA-TECDOC-1355 Security of radioactive sources Interim guidance for comment, June 2003.
6- IAEA-TECDOC-1344 Categorization of radioactive sources Revision of IAEA-TECDOC-1191, Categorization of radiation sources July 2003.

Journal of Physical Security 3(1), 17-35 (2009).

A MODEL FOR HOW TO DISCLOSE PHYSICAL SECURITY VULNERABILIES*

Roger G. Johnston, Ph.D., CPP
Vulnerability Assessment Team
Argonne National Laboratory

ABSTRACT

When security vulnerabilities are discovered, it is often unclear how much public disclosure of the vulnerabilities is prudent. This is especially true for physical security vis a vis cyber security. We never want to help the "bad guys" more than the "good guys", but if the good guys aren't made aware of the problems, they are unlikely to fix them. This paper presents a unique semi-quantitative tool, called the "Vulnerability Disclosure Index" (VDI), to help determine how much disclosure of vulnerabilities is warranted and in what forum. The VDI certainly does not represent the final, definitive answer to this complex issue. It does, however, provide a starting point for thinking about some of the factors that must go into making such a decision. Moreover, anyone using the VDI tool can at least claim to have shown some degree of responsibility in contemplating disclosure issues.

INTRODUCTION

Vulnerability Assessors and others who discover vulnerabilities in physical security devices, systems, measures, or programs often face difficult decisions about whom to warn, when, and in how much detail. When a formal vulnerability assessment (VA) has been chartered, the sponsor of the VA often owns the findings. Proprietary ownership of a VA study, however, doesn't automatically end the matter, it just brings additional people into the conundrum. Furthermore, it doesn't even necessarily relieve the vulnerability assessors of their responsibility to society to warn of clear and present danger.

When a particular vulnerability is unique and isolated within a single, small organization, a public disclosure is probably unwise. Many security vulnerabilities, however, are very extensive and global. The Vulnerability Assessment Team[1] (VAT) at Argonne National Laboratory, for example, has discovered fundamental vulnerabilities in a number of different physical security devices, systems, measures, and programs that could potentially have wide ranging implications for many individuals and organizations. The VAT has demonstrated serious vulnerabilities (as well as potential countermeasures) associated with the use of tamper-indicating seals[2,3,4], radio frequency identification tags (RFIDs) and contact memory buttons[3], Global Positioning System (GPS) receivers[3,5,6], nuclear safeguards[7,8,9], and techniques for vulnerability assessments[10]. It has often been unclear who should be warned of these vulnerabilities and in what detail, even given existing government rules, regulations, classification guidelines, and policies for dealing with sensitive information.

In the world of computer software, security vulnerabilities can typically be dealt with in a more straightforward manner. When a new cyber vulnerability is discovered, it is widely considered best

*Editor's Note: This paper was not peer reviewed.

practice to keep the vulnerability quiet until the software developer or computer manufacturer can be (quickly) contacted, and allowed time to fix the problem.[11,12,13,14] The software upgrade that results can then be rapidly and easily disseminated via the Internet to customers. Indeed, computer and network users know they should frequently (or even automatically) check for software patches and upgrades.

With physical security hardware or procedures in contrast, there is usually no equivalent simple, inexpensive way to provide updates and security fixes, nor even to contact customers. Many physical security devices and systems are sold through a complex network of dealers, vendors, and integrators. The purchaser may even be several layers removed from the end-user. And unlike software fixes, security upgrades to physical security devices, systems, measures, and programs often take a long time to develop and install, and can be quite expensive. Meanwhile, physical security may be at great risk.

Another complicating factor for physical security is that vague, generalized warnings about security vulnerabilities rarely result in countermeasures being implemented. Security managers and security programs tend to be inherently cautious and traditionalist, and are often severely restricted in terms of budget. Typically, attacks must be thoroughly described or demonstrated in detail, along with possible countermeasures, before either the vulnerability will be acknowledged, or any security improvements will be seriously considered. Unfortunately, implementing a countermeasure is often viewed by bureaucratic organizations as an admission of past negligence on the part of security managers, so security managers are often—understandably—less than eager to make changes[11,15,16,17]

With any detailed disclosure of vulnerabilities, we must worry about helping the "bad guys" (nefarious adversaries) more than the "good guys" (security providers). This is especially a concern if—as often happens—security managers or programs ultimately fail to implement recommended security countermeasures. Common reasons for this include a lack of funding, commitment, follow-through, or support from superiors, or an unwillingness to be proactive about security or to admit that security vulnerabilities exist. Sometimes the only way that necessary security countermeasure will be implemented (particularly within government organizations) is if there is public pressure to improve security. But detailed, public discussion of security problems is often a prerequisite for this kind of public awareness and pressure.

The purpose of this paper is to provide a tool to help decide if and how security vulnerabilities should be disclosed. This tool, called the Vulnerability Disclosure Index (VDI), is not presented here as the ultimate, authoritative method for dealing with this complex issue. It is offered instead as a first step, and as a vehicle for thinking about and discussing some of the factors that need to be pondered when vulnerability disclosures are being considered.

The VDI tool is a semi-quantitative method. A high VDI score suggests that public or semi-public disclosure of the vulnerability in at least some detail may well be warranted. A medium score supports the idea that it would be appropriate to discuss the vulnerability, but perhaps in lesser detail and/or to a more limited audience of security professionals and end-users. A low VDI score indicates the vulnerability should probably be kept in confidence, or shared discretely only with those having an explicit and immediate need to know.

THE VDI TOOL

The Vulnerability Disclosure Tool (VDI) works by considering 18 different factors (A-R), and subjectively scoring each for the vulnerability in question. The higher the score for each factor, the greater that factor supports full public, detailed disclosure.

The tables of points appearing below for each factor A-R are meant to serve as a guide to help the user decide on a score. Users should feel free to choose any integer number of points for each factor between the minimum and maximum given in each table. (Thus, users are not restricted to just the values shown in the table.) Scores are meant to be roughly linear, i.e., if a factor doubles in quantity or intensiveness, the number of points assigned to it should approximately double.

One of the most important factors involved in decisions about vulnerability disclosures has to do with the characteristics of the good guys and the bad guys. Factors C-M, P, & Q attempt to deal with this.

Exactly who constitute the "good guys" and who are the "bad guys" should usually be clear from the context. Note, however, that the good guys will often not be 100% good (few government agencies are, for example), nor do the bad guys necessarily have completely malicious goals. For example, while the tactics and extremism of eco-terrorist may well be nefarious, their fundamental concern—protecting natural resources—is not necessarily evil. We should also be careful not to automatically assign "good guy" status to government or authoritarian organizations. A totalitarian regime that uses security measures to suppress its citizens and their civil liberties, for example, does not deserve the title of "good guys".

It is often the case that knowledge of security vulnerabilities is of more help to the good guys than to their adversaries. This is because the good guys usually outnumber the bad guys. (There are, for example, far more bank employees than there are people who are currently active as bank robbers.) Moreover, bad guys usually need to stumble upon only one vulnerability for one target, and can often attack at the time of their own choosing. Security managers, on the other hand, must deal with many vulnerabilities and many possible targets, often extended in time and space. They must even try to manage unknown vulnerabilities. Furthermore, while the bad guys usually fully understand the good guys, the identity of the bad guys is unknown for many security applications. Given this asymmetry between good and bad guys, vulnerability information frequently has more marginal value to the good guys than to the bad guys.

FACTOR A: RISK (0-300 POINTS)

Generally speaking, vulnerabilities that represent minimal risk can be publicly discussed in detail without much concern. Worries about helping the bad guys more than the good guys grow as the risk increases. High-risk vulnerabilities are often best discussed with security managers via private channels, if possible.

With the VDI tool, risk is thought of as the product of the probability of an attack succeeding times the seriousness of the consequences. The term "attack" means an attempt by the bad guys to defeat a security device, system, measure, or program by exploiting the vulnerability in question.

Typically, attacks on the government or public welfare will need to be considered more consequential than attacks on private companies or property.

Table A below provides a lookup table for points to assign to factor A based on the probability of an attacking succeeding, as well as the seriousness of its consequences.

Table A - Factor A, Risk.

Consequences ↓ Probability of attack succeeding ------>

	negligible	low	medium	high	very high
negligible	300	250	200	150	100
low	250	206	162	119	75
medium	200	162	125	88	50
high	150	119	88	56	25
very high	100	75	50	25	0

FACTOR B: OBVIOUSNESS OF THE VULNERABILITY (0-200 POINTS)

If the vulnerability is blatantly obvious to almost any reasonably resourceful person, or if similar attacks have already been suggested publicly thereby making them obvious, there is little point in keeping quiet. Motivated bad guys can figure out obvious vulnerabilities on their own, anyway. If, on the other hand, there has been no previous speculation on this or related vulnerabilities, and only extraordinarily creative, knowledgeable, and clever individuals can figure it out after extensive thought and experimentation, it may well be smart to limit public or detailed discussion of the vulnerability and how to exploit it. (The vulnerability assessors themselves will know if discovering the vulnerability required extensive time and effort, or whether it was spotted almost immediately.)

Security managers often fail to recognize even obvious vulnerabilities—presumably because they are not mentally predisposed to doing so.[2,10]

Table B - Factor B, Vulnerability Obviousness.

obviousness of the vulnerability	points
none	0
a little	50
some	100
a lot	150
very substantial	200

FACTOR C: ATTACK TIME, COST, AND MANPOWER (0-100 POINTS)

If the attack is trivial to prepare, rehearse, and execute—though not necessarily to think up (Factor B)—then a detailed public discussion may be unwise. On the other hand, if few adversaries can marshal the necessary resources, the risk associated with a public disclosure may be minimal.

For this factor, if some of the sub-factors (time, cost, and manpower) are needed in large quantities but others are not, score each separately from 0-100 points, then average them together to get the net score.

If the conditions for preparing and practicing the attack are considerably different from that for executing the attack, consider which is the more important constraint for the given vulnerability, and choose the score for factor C accordingly. (Some attacks, for example, must be executed quickly to be effective, but may take months for preparation and practice.)

Table C - Factor C, Attack Time/Cost/Manpower.

time, cost, & manpower for practice & execution	points
very minimal	0
minimal	25
some	50
a lot	75
very extensive	100

FACTOR D: LEVEL OF SKILL, SOPHISTICATION, AND HIGH TECHNOLOGY (0-100 POINTS)

If the average person on the street can easily exploit the vulnerability, a public airing of details may be unwise. On the other hand, if only highly trained, sophisticated adversaries can pull off the attack, and only after extensive practice with expensive high-tech or social engineering tools, there is probably minimal harm in discussing the attack in some detail. This will allow security managers to better appreciate the problem—and be motivated to fix it.

Attacks on some security devices require great skill, but little technological expertise. (Picking a lock is an example.) If some of the sub-factors (skill, sophistication, and level of technology) are high, but others are low, score each separately from 0-100 points, then average them together to get the net score for this factor.

Table D - Factor D, Attack Skill/Sophistication/High-Technology.

required skill, sophistication, & high-technology	points
very minimal	0
minimal	25
some	50
a lot	75
very extensive	100

FACTOR E: COST, TIME, AND COMPLEXITY OF THE COUNTER-MEASURES OR ALTERNATIVE SECURITY (0-200 POINTS)

If the suggested countermeasures are cheap and easy, a full public disclosure of both the vulnerability and the countermeasures may be warranted. If, however, there are no known countermeasures or alternatives, or they are impractical, expensive, and/or time consuming to put in place, there is typically little chance they will be widely implemented. Being discreet about the vulnerability is therefore indicated. (There is the chance, of course, that somebody else might be able to devise more practical countermeasures if she were made aware of the vulnerability.)

Table E - Factor E, Countermeasures.

cost & complexity of countermeasures	points
very high (or there are no countermeasures)	0
fairly high	50
moderate	100
fairly low	150
very low	200

FACTOR F: RATIO OF CURRENT TO FUTURE USE (0-100 POINTS)

This factor considers the ratio of current use of security to the extent of use likely in 3 years. If the security device, system, measure, or program hasn't been fielded to any great extent, there should be ample time and at least some willingness to fix problems, so a public discussion of vulnerabilities may be warranted. If, on the other hand, the fixes would mostly have to be retrofitted in the field, the odds that this will actually happen is less, and a detailed public disclosure of vulnerabilities may be risky.

Table F - Factor F, Ratio of Current Use of the Device, System, or Program to Use 3 Years in the Future.

ratio of current to future use	points
>5	0
2-5	25
0.5-2	50
0.2-0.5	75
<0.2	100

FACTOR G: NUMBER OF ORGANIZATIONS FOR WHICH THE VULNERABILITY IS RELEVANT (0-200 POINTS)

If the vulnerability is highly localized, e.g., the local ice cream shop has a vulnerability because the manager frequently forgets to lock the back door at night, it clearly makes little sense to widely publicize the vulnerability and alert the bad guys. The vulnerability should quietly be pointed out to the manager or shop owner. If, on the other hand, the vulnerability is shared by a large number of diverse organizations, a public disclosure may be prudent.

The reasons this factor is not the sole, overriding consideration in vulnerability disclosures include the following:

1. We cannot always be 100% certain exactly how many organizations may actually be subject to a given vulnerability.
2. Going public can potentially contribute to better security for organizations and security applications we have not considered. For example, publicly discussing the ice cream shop's vulnerability may remind other unrelated businesses to lock their doors at night.
3. Going public may also help ensure good security practice at future ice cream shops and unrelated businesses that don't currently exist. (Factor G.)
4. Even if we try to carefully channel the vulnerability information by disclosing it to just one or a small number of organizations, there is still a risk that the information will leak out anyway, especially if the organization(s) are large and/or have a poor security culture. (Factors H, I, L, & M.)
5. A public disclosure may pressure the ice cream shop into implementing better security than if the issue is just discussed privately.
6. Even if only one or a small number of organizations are relevant, a public disclosure is relatively safe if the security of those organizations is poor in other ways than just the vulnerability in question. (Factors L & M.)

Note: When there are no relevant organizations, the physical security device, system, measure, or program in question is not in use. Thus, full public disclosure (200 points in the first row) in warranted for factor G because there is no immediate risk.

Table G - Factor G, Number of Vulnerable Organizations

number of organizations	points
0	200
1	0
2 or 3	20
4-9	50
10-20	90
20-50	140
50-100	180
100-200	190
>201	200

FACTOR H: NUMBER OF SECURITY PERSONNEL (0-100 POINTS)

This factor concerns how many people inside the good guys' organizations will ultimately learn about the vulnerability if management is informed. (For many organizations, this nearly equals the number of total security employees, because few organizations are good at compartmentalizing information for any length of time.) The larger the number of people involved, the more likely the vulnerability will be deliberately or inadvertently leaked anyway, so the lower the risk of going public with the vulnerability in the first place.

Table H - Factor H, Number of Security Personnel

typical size of good guys' security force	points
very small	0
small	25
medium	50
large	75
very large	100

FACTOR I: RATIO OF GOOD GUYS TO BAD GUYS (0-200 POINTS)

When good guys greatly outnumber bad guys, openly sharing vulnerability information tends to do more good than harm. For example, there are probably more child care providers than there are pedophiles at risk for molesting children. Thus, publicly providing information on how to protect children is probably prudent. On the other hand, in the case of underage drinkers, there are likely to be more minors interested in illegally obtaining alcohol than there are store clerks and bar bouncers to check IDs, so it may make more sense to disclose vulnerabilities directly to alcohol vendors than to the general public.

Note that for Factor I, only personnel directly involved in relevant security operations should be considered—not the total number of general employees.

Table I - Factor I, Ratio of Good to Bad Guys

ratio of good guys to bad guys	points
<< 1	0
< 1	50
~ 1	100
> 1	150
>> 1	200

FACTOR J: THE ADVERSARY IS KNOWN (0-100 POINTS)

If the bad guys are well known, it may be prudent to carefully direct the flow of vulnerability information away from them. On the other hand, when the identity of the bad guys is largely unknown, e.g., they might even be unknown insiders within the security organization, we have less of an opportunity to effectively direct the flow of vulnerability information. A public disclosure is then more warranted.

Table J - Factor J, Bad Guys Identity.

how well the bad guys are known	points
fully identified	0
fairly well known	25
somewhat known	50
slight idea	75
total mystery	100

FACTOR K: THE DEGREE TO WHICH THE SECURITY DEPENDS ON SECRECY (0-100 POINTS)

Secrecy is not usually a good long-term security strategy. [18] That's because people and organizations are typically not very good at keeping secrets. Thus, if security is largely based on a misplaced faith in secrecy, taking actions to end over-reliance on secrecy could actually be healthy.

A public discussion of vulnerabilities may force good guys who rely mostly on secrecy to implement better security measures. It is, for example, believed that publicly discussing software vulnerabilities forces manufacturers to fix security problems faster and better.[11,19] In any event, holding private discussions with security managers who rely mostly on secrecy is unlikely to result in improved security because they will (at least in the author's experience) tend to foolishly count on the vulnerability remaining a secret.

Table K - Factor K, Secrecy.

security is primarily based on secrecy	points
not at all	0
just a little	25
some	50
a lot	75
completely	100

FACTOR L: THE EFFICACY OF THE OTHER SECURITY MEASURES (0-120 POINTS)

If an organization has extremely poor general security, there are already multiple vulnerabilities to exploit. Thus, the risk from a public disclosure of a single vulnerability is greatly lessened. Moreover, a public disclosure might pressure the good guys into improving overall security, not just deal with the immediate vulnerability in question. If, on the other hand, the security is generally outstanding except for the sole problem(s) that have been identified, a public disclosure might help the bad guys succeed where they would otherwise have failed.

Table L - Factor L, Overall Security Effectiveness.

overall effectiveness of security	points
excellent	0
good	30
fair	60
poor	90
very poor	120

FACTOR M: THE SOPHISTICATION OF THE GOOD GUYS (0-300 POINTS)

When security managers and other security personnel don't fully understand the security devices, systems, or programs they are using, and lack awareness of the important vulnerabilities, we are probably better off being very public and detailed in discussing the vulnerability in question. If the good guys think no vulnerabilities are even possible—a distressingly common situation in the field of physical security—this factor should be assigned a large number of points.

Table M - Factor M, Security Sophistication

sophistication of the good guys	points
excellent	0
good	75
some	150
just a little	225
none	300

FACTOR N: "SILVER BULLET" ATTITUDES (0-200 POINTS)

This factor considers the degree to which the security device, system, measure, or program is generally viewed by government, business, end-users, potential end-users, and the public as a security panacea. If the security is thought to magically provide invincible security, a detailed public discussion of the vulnerability is probably healthy. Even though the bad guys might also temporarily believe in the myth of invincibility, the good guys cannot count on this indefinitely because the bad guys will tend to think more critically about security vulnerabilities than the good guys.

Examples of security technologies that have clearly been viewed—quite incorrectly—as "silver bullets" (panaceas) include RFIDs, GPS, biometrics, encryption, and tamper-indicating seals.[3]

Table N - Factor N, Panacea & Overconfidence Illusions.

security is viewed as as largely invincible	points
not at all	0
a little	50
some	100
a lot	150
completely	200

FACTOR O: THE EXTENT OF OVER-HYPING (0-120 POINTS)

If the security device, system, measure, or program is being over-hyped by manufacturers, vendors, or other proponents, a detailed public discussion of the vulnerabilities is probably healthy and will ultimately result in better security. Over-hyping is a serious problem for physical security because of the relative lack of rigorous standards, metrics, principles, and testing guidelines, as well as effective research & development.[2,9,10]

Symptoms of over-hyping include sloppy terminology, or exaggerated and absolutist phrases such as "tamper-proof", "completely secure", "*impossible* to defeat", "passed all vulnerability assessments". Other indications of over-hyping are the misuse or misrepresentation of statistics and tests, deliberate obfuscation, or comparing apples and oranges.[2]

Table O - Factor O, Over-Hyping.

amount of over-hyping	points
none	0
a little	30
some	60
a lot	90
completely	120

FACTOR P: HOW MUCH ARE THE BAD GUYS LIKELY TO BENEFIT? (0-120 POINTS)

If the bad guys have (or believe they have) little to gain from exploiting a vulnerability, then there is probably little risk to a full public discussion. Of course, what the bad guys hope to gain depends on the context. Crooks would be interested in economic gain, disgruntled individuals in retaliation, terrorists in disruption and death, radicals in making political statements, hackers in demonstrating prowess, and vandals in entropy.

This factor deals with how the bad guys can benefit, whereas the factor A (risk) dealt with how much the good guys have to lose (and the probability).

Table P - Factor P, Bad Guys Benefit.

bad guys stand to gain	points
a tremendous amount	0
a lot	30
some	60
just a little	90
nothing	120

FACTOR Q: HOW SUBSTANTIAL ARE THE PENALTIES TO BAD GUYS IF THEY ARE CAUGHT? (0-80 POINTS)

Some illegal activities, such as product counterfeiting or copyright violations, carry relatively light legal penalties, or else the laws are rarely enforced. If the bad guys face little risk from exploiting a vulnerability, they may be more likely to proceed. A public disclosure of the vulnerability is therefore more risky.

Table Q - Factor Q, Penalties.

extent of likely penalties	points
negligible	0
a little	20
some	40
a lot	60
very substantial	80

FACTOR R: MOTIVATION OF THE INDIVIDUALS CONTEMPLATING A VULNERABILITY DISCLOSURE (0-160 POINTS)

While good things can be done for bad reasons, and vice versa, it is worth considering the motivation of the would-be discloser. If he or she wants to disclose the existence of vulnerabilities primarily for selfish reasons, it might be prudent to exert at least a partial restraint on full disclosure. Obvious conflicts of interest need to be considered as well, e.g., the vulnerability assessors are evaluating a product made by a competitor of their employer.

This factor requires the VDI tool user to attempt to gauge motivation. If the vulnerability assessor himself is using the tool, he will need to undertake a certain amount of honest introspection that may be healthy when considering disclosure issues.

Table R - Factor R, Assessor Motivation.

motivation	points
entirely self-promotion or self-interest; major conflict of interest	0
partially self-promotion or self-interest	40
a mix of self-interest and altruism	80
mostly altruistic	120
entirely altruistic; zero conflict of interest	160

INTERPRETATION

The overall VDI score is computed as follows. The sum of the points from all the factors (A-R) is computed, then normalized to (divided by) the maximum possible number of points (2800), and finally multiplied by 100 to produce a VDI value in percent. The higher the VDI percent, the more appropriate it is to widely disseminate detailed information about the vulnerability in question. Thus, VDI in percent = [Σ(scores for factors A through R) / 2800] x 100%

The recommendations that the model makes for various VDI scores are shown in table S. The term "fully enabling" means enough detail about the vulnerability is presented to allow anyone sufficiently qualified to reproduce a viable attack on the relevant security device, system, measure, or program with minimal effort. "Partially enabling" means only incomplete information is provided, while "not enabling" means the disclosure provides little practical guidance to an adversary about exactly how to exploit the discovered vulnerability.

Table S - Recommended Course of Action Based on VDI Scores.

VDI score	Recommended level of vulnerability disclosure
>75%	public release, fully enabling
68%-75%	public release, partially enabling
60%-67%	public release, non-enabling
50%-59%	restricted release (security trade journals & meetings), fully enabling
40%-49%	restricted release (security trade journals & meetings), partially enabling
34%-39%	restricted release (security trade journals & meetings), non-enabling
12%-33%	highly restricted, private release: contact the relevant good guys directly
<12%	no disclosure at all

Note that for VDI scores in the range 34%-59%, the recommendation in table S is for disclosure, but only to an audience of security professionals. This can be done by using security trade journals and security conferences. While such forums cannot be guaranteed to be free of bad guys, they probably have a higher ratio of good guys to bad guys than would be the case for the general public.

It is also important to bear in mind that the recommended choice of action from table S does not automatically preclude those actions listed below it in the table. For example, if the VDI score calls for a non-enabling public disclosure of the vulnerability, this does not preclude more detailed, enabling discussions in private with good guys at a later time. The publicity surrounding the disclosure of a vulnerability (even if non-enabling) may elicit inquiries from good guys who have a legitimate need to know more details. The typical problems with vague public disclosures, however, are that (1) they may not reach the most important audience, and (2) they may not be taken seriously if details or demonstrations are not provided.

EXAMPLES

Five examples are presented in this section, with 1-3 being hypothetical. These 5 examples are used to check whether the guidance offered by the VDI index is reasonable. At least in the author's view, the recommended courses of action that come from the VDI tool seem sensible for all 5 examples. This, however, is far from a rigorous validation of the model.

Table T shows the points assigned to each factor for the 5 examples, as well as the total points and the resulting VDI scores.

Example 1: The mascot for Dunderhead State University is a billy goat. Loss or harm to the mascot could cause serious damage to the University's pride, and undermine the morale of the Fighting Scapegoats football team and their supporters. A subtle vulnerability has been discovered in the security provided for the mascot, making it very easy for students and fans from competing schools to kidnap or otherwise harm the mascot. Fixing the problem is possible, but complicated. The vulnerability is unique to Dunderhead State and the one location where the mascot is kept. The overall VDI percentage computed from Table T is 29%, indicating (from table S) that we should discuss the matter only with University students and staff responsible for the mascot's security and welfare. A public disclosure would be imprudent.

Example 2: A simple but non-obvious method is found for stealing candy bars from vending machines. The attack can be eliminated by quickly snapping a cheap piece of plastic into the interior of the machine the next time it is refilled. From table T, the overall VDI score is 44%, indicating (from table S) that we should do a partially enabling disclosure to security professionals and vending companies, including possibly some discussion of the countermeasure.

Example 3: A (widely respected) company hired by many organizations to perform background checks on security personnel is discovered to have done poor quality work, and may even have faked much of the data. The company's competitors do not seem to have this problem, though switching vendors is somewhat expensive. The overall VDI percentage in table T is 51%, indicating that we should do a fully enabling disclosure to general security professionals about the problem, probably going so far as to even identify the company.

Example 4: Lawrence M Wein raised a controversy about whether a paper discussing terrorist poisoning of milk with botulinum toxin should be openly published.[20,21] Here, we will assume that this theoretical attack would have major consequences, but a relatively low probability of success[22]. In addition, we shall assume—as Leitenberg and Smith maintain[22]—that a terrorist would need considerable sophistication, skill, time, and effort to obtain significant quantities of the botulinum toxin. Under these assumptions and the author's view of the situation (which may or may not be correct), table T shows an overall VDI percentage of 62%, indicating that the vulnerability should be discussed openly in a non-detailed manner. Given that the paper itself is not very enabling[22], this is essentially what the National Academy of Sciences actually decided to do when it chose to publish the paper despite government objections.[23]

Example 5: The VAT has demonstrated how easy it is for relatively unsophisticated adversaries to spoof—not just jam—civilian GPS receivers using widely available commercial GPS satellite simulators.[5,6] Unlike the military signal, the civilian GPS signal is not encrypted or authenticated. Even though it was never designed for security applications, it is frequently used that way. Most GPS users are unaware of the vulnerability. Prior to developing the VDI tool, the VAT made the decision to publicly disclose the vulnerability. This disclosure was partially enabling in that the use of a GPS satellite simulator was discussed. After developing the VDI tool, the VAT scored the GPS vulnerability as shown in Table T. The VDI score of 69% supports our prior intuitive decision to do a partially enabling public release.

Table T - Scores for Each VDI Factor for the 5 Examples.

	Example 1 (mascot)	Example 2 (candy bars)	Example 3 (bkg checks)	Example 4 (toxic milk)	Example 5 (GPS)
Factor A	130	119	56	119	60
Factor B	25	20	25	150	100
Factor C	25	10	10	75	60
Factor D	25	10	5	75	60
Factor E	40	190	110	120	150
Factor F	50	50	65	45	100
Factor G	0	200	200	200	200
Factor H	10	50	80	20	80
Factor I	50	0	60	195	180
Factor J	25	95	50	90	90
Factor K	70	5	90	20	40
Factor L	10	40	60	70	60
Factor M	70	110	150	150	290
Factor N	100	50	150	110	195
Factor O	10	10	90	75	115
Factor P	70	90	50	60	35
Factor Q	20	30	50	70	40
Factor R	80	140	120	80	80
Sum of Points	810	1219	1421	1724	1935
VDI	29%	44%	51%	62%	69%

DISCUSSION

The VDI score computed in this model is meant to provide guidance on the maximum amount of vulnerability information (if any) that should be disclosed. Generally, it is prudent to release no more information about a vulnerability to no more people than is necessary to accomplish what needs to be done, i.e., alert security managers to a problem, create more realistic views about security, and/or get countermeasures implemented. Minimizing the amount of information and the people who receive it reduces the odds that it will benefit the bad guys—but, as discussed above, it also reduces the odds that the good guys will take necessary actions.

At best, the VDI tool should be considered only a preliminary attempt to encourage thinking and discussion of vulnerability disclosure issues. The tool cannot be the final arbitrator for whether to disclose security vulnerabilities, in what degree of detail, when, or to whom. Every case is different, and there are other, sometimes overriding factors that must also be considered but are missing from the VDI model. These include government classification regulations, state and federal laws, organizational & employer rules, proprietary and intellectual property issues, legal liabilities[24], contractual obligations such as who sponsored the vulnerability assessment and who owns its results, and personal views on morality, fairness, and social responsibility. The author of this paper and the VDI tool can make no claim to any unique insight or wisdom on any of these matters.

There are other limitations to this tool as well. While the various factors (A-R), their scoring, and relative weights seem plausible, it is very difficult to rigorously defend specific details of the VDI tool. Questions very much open for debate include:

- What factors are missing?
- What factors A-R are correlated or "non-orthogonal" and should be combined into some other, more general factor?
- Are the relative weights of the factors (i.e., the maximum possible number of points for each factor) appropriate?
- Does the roughly linear assignment of points in the table for each factor make sense?
- Should the recommended course of action for the various ranges of VDI scores in table S be different? (Admittedly the break points in column 1 of table S are somewhat arbitrary.)

In terms of weighting, the factor weights are as follows:
A=M > B=E=G=I=N > R > L=O=P > C=D=F=H=J=K > Q.
This weighting, while very much open for debate, is not arbitrary. In the view of the author, the factors with the highest possible scores (or weights) probably are indeed the most critical.

It also is very important to avoid the "fallacy of precision". This is thinking that because one has assigned numeric values to complex parameters, then he or she automatically has a rigorous understanding of them. The fact is that quantified ambiguity is still ambiguity.

Despite the myriad potential problems with the VDI tool, it does nevertheless serve as a means for raising many of the critical issues associated with the disclosure of vulnerabilities. Anyone conscientiously using the tool automatically demonstrates that he or she has at least made a rudimentary attempt towards sincerely considering the risks and implications of disclosing vulnerabilities. The VDI score can help to justify the decision to disclose or not to disclose. As such, the tool may be of some value for protecting vulnerability assessors and others from the retaliation and recrimination that all too commonly arises when vulnerability issues or questions about security are raised in good faith.[10,11,15,1625] The VDI tool might also help the user choose a more appropriate channel, medium, or forum for vulnerability disclosures than he or she might be otherwise inclined to pursue, e.g., the popular press or the Internet vs. security conferences and journals vs. private discussions with manufacturers or end-users.

REFERENCES

[1] Vulnerability Assessment Team Home Page, http://www.ne.anl.gov/capabilities/vat.
[2] Roger G. Johnston, "Assessing the Vulnerability of Tamper-Indicting Seals", Port Technology International 25(2005): 155-157.
[3] Roger G. Johnston and Jon S. Warner, "The Dr. Who Conundrum", Security Management 49(2005): 112-121.
[4] Roger G. Johnston, Anthony R.E. Garcia, and Adam N. Pacheco, "Efficacy of Tamper-Indicating Devices", Journal of Homeland Security, April 16, 2002, http://www.homelandsecurity.org/journal/Articles/displayarticle.asp?article=50.
[5] Jon S. Warner and Roger G. Johnston, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing", Journal of Security Administration 25(2002): 19-27.
[6] Jon S. Warner and Roger G. Johnston, "GPS Spoofing Countermeasures", Homeland Security Journal, December 12, 2003, http://www.homelandsecurity.org/bulletin/Dual%20Benefit/warner_gps_spoofing.html.
[7] Morten Bremer Maerli and Roger G. Johnston, "Safeguarding This and Verifying That: Fuzzy Concepts, Confusing Terminology, and Their Detrimental Effects on Nuclear Husbandry", Nonproliferation Review 9(2002): 54-82, cns.miis.edu/pubs/npr/vol09/91/91maerli.pdf.
[8] Roger G. Johnston and Morten Bremer Maerli, "International vs. Domestic Nuclear Safeguards: The Need for Clarity in the Debate Over Effectiveness", Disarmament Diplomacy, issue 69, February-March 2003, http://www.acronym.org.uk/dd/dd69/69op01.htm.
[9] Roger G. Johnston and Morten Bremer Maerli, "The Negative Consequences of Ambiguous 'Safeguards' Terminology", INMM Proceedings, July 13-17, 2003, Phoenix, AZ.
[10] Roger G. Johnston, "Effective Vulnerability Assessments", Proceedings of the Contingency Planning & Management Conference, Las Vegas, NV, May 25-27, 2004.
[11] Bruce Schneier, "Is Disclosing Vulnerabilities a Security Risk in Itself?", InternetWeek, November 19, 2001, http://www.internetweek.com/graymatter/secure111901.htm.
[12] M. Rasch, "'Responsible Disclosure' Draft Could Have Legal Muscle", SecurtyFocus, November 11, 2002, http://online.securityfocus.com/columnists/66.
[13] A. Arora, R. Krishnan, A. Nandkumar, R. Telang, and Y. Yang, "Impact of Vulnerability Disclosure and Patch Availability—An Empirical Analysis", April 2004, http://www.dtc.umn.edu/weis2004/telang.pdf.
[14] A. Arora and R. Telang, "Economics of Software Vulnerability Disclosure", Security & Privacy 3(2005): 20-25.
[15] E. Hall, "Risk Management Map", Software Tech News 2(2004), http://www.softwaretechnews.com/technews2-2/stn2-2.pdf.
[16] M.A. Caloyannides, "Enhancing Security: Not for the Conformist", Security & Privacy 2(2004): 86-88.
[17] Roger G. Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", Nonproliferation Review 8(2001): 102-115, http://www.princeton.edu/~globsec/publications/pdf/9_2johnston.pdf.
[18] Roger G. Johnston, "Cryptography as a Model for Physical Security", Journal of Security Administration 24(2001): 33-43.
[19] A. Arora, R. Telang, and H. Xu, "Timing Disclosure of Software Vulnerability for Optimal Social Welfare", November 2003, http://www.andrew.cmu.edu/user/xhao/disclosure.pdf.
[20] Lawrence M. Wein, "Got Toxic Milk", New York Times, May 30, 2005, http://www.nytimes.com/2005/05/30/opinion/30wein.html?ex=1275105600&en=e56b2b8b96d56f1e&ei=5088.

[21] Rebecca Carr, "Publication Heeds U.S., Pulls Terror Article", Atlanta Journal and Constitution, June 26, 2005, http://www.ajc.com/hp/content/auto/epaper/editions/sunday/news_24ebc541731e70fe0050.html.
[22] M. Leitenberg and G. Smith, "'Got Toxic Milk?': A Rejoinder", (2005), http://www.fas.org/sgp/eprint/milk.html.
[23] Scott Shane, "Paper Describes Potential Poisoning of Milk", New York Times, June 29, 2005, http://www.nytimes.com/2005/06/29/politics/29milk.html?ex=1277697600&en=06b46176c5d1a2cf&ei=5088&partner=rssnyt&emc=rss.
[24] J. Stisa Granick, "Legal Risks of Vulnerability Disclosure", (2005), http://blackhat.com/presentations/win-usa-04/bh-win-04-granick.pdf.
[25] Anonymous, "Don't Shoot the Messenger", CSO 5(2006): 52-53, http://www.csoonline.com/read/080106/col_undercover.html.

Journal of Physical Security 3(1), 36-39 (2009)

Viewpoint Paper

Confidentiality & the Certified Confidentiality Officer: Security Disciplines to Safeguard Sensitive/Critical Business Information

John Kanalis CCO, CPO, CSSMP, CPOI
Business Espionage Controls & Countermeasures Association (BECCA)
BECCA Europe Administrator

Introduction

Confidentiality is the ethical and professional duty not to disclose inappropriate information to a third party. Confidentiality may apply because of the legal or ethical requirements of certain professionals, such as those who hold Certified Confidentiality Officer (CCO) certification (See http://www.becca-online.org/ccoprogram.html) In business, confidentiality exists to protect the privacy of a business entity, including its critical or sensitive business information. Policies and procedures are needed to safeguard against espionage and/or intentional or unintentional disclosure of sensitive or proprietary information. These policies and procedures may be mandated by laws or regulations, or by the professional ethical obligations of employees. These policies and procedures may also be implemented as a best practice to help decrease insider or outsider access to critical business information.

The lack of preplanning regarding the flow of confidential information within the business environment can result in misunderstandings about safeguarding critical business secrets and preventing thefts of intellectual property, including property protected by copyrights, trademarks, and patents. (See www.BECCA-online.org)

A confidentiality vulnerability audit is an initial step to business's minimum requirements of being protected against danger or loss. (See John Kanalis, 2008, BECCA Training in Business Espionage Controls & Countermeasures). This is a fact-finding, non-fault-finding audit that involves:

- a search for vulnerabilities through information collection and analysis, and
- a way to identify leaks, sources, & indicators potentially exploitable by an adversary;

There are a number of reasons why business confidentiality can be important. These include:
-Trade secrets and intellectual property often need to be kept from business competitors.
-The improper dissemination of information about current business objectives or future projects may harm the business.
-Confidentiality may be necessary for employee security, and for the security of their families.
-Job security can be an issue.
-Confidentiality provisions may help to encourage employees to make use of services designed to help them, such as counselling or other employee assistance programs.

-Assurance of confidentiality may make it easier people to seek help without fear or damage to reputation or other relationships.

Confidentiality is based on four basic principles:
1. Respect for a business's right to privacy.
2. Respect for human relationships in which business information is shared.
3. Appreciation of the importance of confidentiality to both the business and its employees.
4. Expectations that those who pledge to safeguard confidential information will actually do so.

Confidentiality is necessary for the best interests of the organization, or because disclosure of the information will cause significant damage to the business itself or to other organizations. The need for confidentiality exists when information is designated as "confidential" (e.g. stamped or announced). It also applies where the need for confidentiality is obvious or evident (depending on the nature of the material or context of the situation), or when required by applicable law—even when the information is not specifically designated as confidential.

Typically, it is not solely up to the individual to determine what is and is not confidential. If the organization considers and treats information as confidential, then officials and employees of the organization must respect that need for confidentiality. Moreover, individuals must not be permitted to arbitrarily overrule or disregard their duty to maintain confidentiality.

Business officials and employees are often legally required to keep certain business and personal information confidential. This legal obligation exists even if officials and employees have not signed contracts or other documents related specifically to confidentiality.

Board members in particular have been placed in a position of trust, and it is their fiduciary responsibility to honour the business's need to keep certain information confidential. A Board member or employee who discloses confidential information can create significant legal liability for the organization if he/she is legally required to maintain confidentiality. The Board member or employee may also face personal liability as a result of disclosing confidential information.

Postulates

I propose here 10 postulates about confidentiality in the business world.

1. The first postulate is that a dynamic security mechanism is needed to prevent losses (loss = cost) that will facilitate the accomplishment of objectives, namely the continued smooth operation of the business while ensuring:
• The security of business structure (both tangible & intangible elements);
• The security of employees and materials;
• The security of information, communications, & information systems that are used to manage risk (risk = intention + ability + opportunity), whether the risk is personal, human, physical, technological, or otherwise has an impact on the organization's well being.

The second postulate is that this security mechanism must, if it is to be effective in managing the foregoing risks and impacts, involve:
• Prevention;

• Tracking;
• Corrective actions.

The third postulate is that the security mechanism needs to be exposed to real-time, tactical assessments that take into account:
• The risk or threat to the whole business;
• The acceptable level of risk or threat;
• The processes of reacting to a threat;
• The need to reduce the overall vulnerability.

The fourth postulate is that this security mechanism, if it is to be effective and produced tangible results, must specifically address:
• Policies for how to implement the security mechanism;
• Procedures detailing the implementation process.

The fifth postulate is that all of the above issues must be integrated into a coherent program, which I call the "Security Program" or "Security Master Plan".

The sixth postulate is that current business risks are linked to each other, creating a complex co-dependency. Thus, the management of initial frontline responses (e.g., guard actions and responsibilities at a building entrance) has passed into the arena of comprehensive security management.

The seventh postulate is that security strategy must determine the procedures for understanding the nature of risk in detail, in addition to specifying the response plan.

The eighth postulate is that the security mechanism must collect and disseminate information about security-related business processes and how the security mechanism may affect profitability, the flow of information, and the reputation of the business.

The ninth postulate is that the security mechanism, if it is to be effective, must analyze recruiting information from different sources (and in collaboration with others), and use this information to help protect the business.

The tenth postulate is that the security mechanism must have planned—in advance—what happens on the next business day after a serious adverse event. The vast majority of organizations and institutions do not anticipate crises or manage them effectively once they have occurred. Neither the mechanics nor the basic skills are in place for effective crisis management (Managing Crises before They Happen – Mitroff, 2001).

Crises and Continuity

The Institute for Crisis Management (www.crisiexperts.com) defines a business crisis as a problem that:

1) Disrupts the way an organization conducts business, and

2) Attracts significant news media coverage and/or public scrutiny. Typically, these crises are dynamic situations that threaten the economics and well-being of the organization and its employees.

Most business crisis situations, such as loss of critical/sensitive business information, may be either sudden or chronic, depending on the amount of advance notice and the chain of events in the crisis. The risk to sensitive and/or critical business information continues to increase significantly as adversaries—both domestic and foreign—focus their espionage resources in even greater numbers on the private sector.

Business continuity can be aided by the use of Sensitive Information Risk Analysis (SIRA) and Evaluation of Sensitive Information (ESA) to reduce and manage the risk of espionage. The development and implementation of rules, policies, procedures, audits, and continuing assessments for the purpose of avoiding the competitive loss of business secrets is an important part of the overall security framework.

Confidentiality applied as a stand-alone process can help identify whether complete pathways exist that link to a potential "window of opportunity".* Conservative assumptions can also be useful to estimate business exposure based on indicators & facts.** Another important element is gaining strong support and commitment to the process from the organization's executive management.

Conclusion

Confidentiality is a prerequisite in any internal or external business transaction. A Certified Confidentiality Officer (CCO) is a security professional who can be of help. He or she has specific knowledge of how to avoid loss, protect critical/sensitive business information, safeguard proprietary information, and enrich a business's awareness and training on confidentiality issues. Moreover, a CCO can integrate into organization's philosophy and culture the idea that the "Nothingness Treaty" (nothing happened yesterday, nothing happened today, nothing will happen tomorrow) is a poor philosophy for protecting an organization and its employees.

---

* See, for example, Roger G. Johnston, "How to conduct an Adversarial Vulnerability Assessment", Vulnerability Assessment Team, Los Alamos National Laboratory, 2006.
** See, for example, E.G. Bitzer and R.G.Johnston, "Creative Adversarial Vulnerability Assessments", Vulnerability Assessment Team, Los Alamos National Laboratory, 2006.