Proceedings of the 51st Annual INMM Meeting
Baltimore, MD, July 11-15, 2010

# HANDBOOK OF SECURITY BLUNDERS

Roger G. Johnston and Jon S. Warner
Vulnerability Assessment Team
Nuclear Engineering Division
Argonne National Laboratory
9700 S. Cass Ave, Building 206, Argonne, IL 60439-4840

## ABSTRACT

We've undertaken hundreds of vulnerability assessments on a variety of different physical security devices, systems, and programs, including those involving nuclear safeguards. In the course of this work, we have repeatedly encountered many of the same kinds of security mistakes or deficiencies across a wide range of security applications. For the last several years, we have undertaken an effort to catalog the most common and serious of these security errors. We have also attempted to devise generic suggestions for avoiding or mitigating these problems. The result is a general catalog of security mistakes and countermeasures that we call "The Handbook of Security Blunders". This paper discusses some of these mistakes and countermeasures that we believe to be most relevant for nuclear security and safeguards.

## INTRODUCTION

In our view, the old adage (and metaphor) that "the chain of security is only as good as the weakest link" has considerable merit. In other words, what you get right about security may be less important than what you get wrong. That's because adversaries don't ordinarily attack at random, but rather at the weakest point(s). We thus believe that recognizing dangerous security mistakes may be more helpful (or at least as helpful) to security managers and practitioners as focusing on strategies, recipes, and procedures for having good security.

As vulnerability assessors, first at Los Alamos National Laboratory (1992-2007) and now at Argonne National Laboratory, we have conducted vulnerability assessments on hundreds of different physical security devices, systems, and programs.[1] These vulnerability assessments have been conducted for private companies, non-government organizations (NGOs), international agencies, and government organizations, and include numerous nuclear safeguards applications.

In conducting this work, we have repeatedly encountered many of the same kinds of security mistakes, deficiencies, or vulnerabilities across a wide range of security applications. For the last several years, we have undertaken an effort to catalog the most common and serious kinds of these security errors. We have also attempted to devise generic suggestions for avoiding or mitigating these problems. The result is an unclassified catalog of generic security mistakes and countermeasures that we call (somewhat flippantly) "The Handbook of Security Blunders". This paper presents some of these security mistakes and potential countermeasures that we believe are most relevant for nuclear security and safeguards, both domestic and international.

## BLUNDERS AND COUNTERMEASURES

We list below common blunders in decreasing order of "significance". We define this (somewhat loosely) as the relative weight of five factors summed together: Our estimation of (1) the extent to which the blunder represents a major philosophical misunderstanding about security; (2) the seriousness of the blunder in terms of potential negative consequences; (3) the likelihood the blunder will be exploited by adversaries; (4) how common the blunder is; and (5) how applicable the blunder is to a wide range of security applications (as opposed to applying only in special situations or applications).

This "seriousness" ranking is subjective and should not be taken overly seriously. Indeed, every security or safeguards application is unique and cannot be fully characterized by general paradigms. Nevertheless, if time and resources limit how many blunders can be addressed for a given security device, system, or program, then blunders early on in the following list probably merit more attention and thought than those later on.

**Blunder 1**: Compliance based security.

Comments: Security professionals are often required to undertake certain security actions or paperwork as required by the organization, the government, laws, rules, regulations, guidelines, traditional practice, auditors, bureaucrats, committees, etc. The need to comply may be unavoidable, but in our experience, it often has little to do with good security. (We estimate that, on average, about 20% of security regulations in large organizations actually make security worse, sometimes dramatically.) Compliance can compromise security by draining resources, being a distraction, turning employees against security, engendering over-confidence, or because the compliance measures are vague, ill-conceived, pedantically enforced, punitive, out of date, or inappropriate for the particular security application or facility in question.

Countermeasures: Security managers and practitioners need to be constantly made aware of the fact that good compliance and good security are not the same thing. The latter is far more important, though the former cannot usually be ignored. An effective security strategy requires viewing compliance as an unavoidable responsibility, but not the central issue in providing effective security. In our view, security managers have a professional and moral responsibility to push back on compliance that is pointless or damaging to security. In many organizations, however, doing so places their career at risk.

**Blunder 2**: Confusing inventory with security.

Comments: Confusing the inventory function with the security function almost always leads to bad security. Inventory is counting and locating assets. It may detect inadvertent errors by innocent insiders, e.g., sending the shipment to the wrong location, but it is not designed to deal with spoofing or deliberate nefarious attacks. That is the job of security.

Time and time again, we have witnessed security professionals and designers (especially those in the field of nuclear security and safeguards) unambiguously state that they understand that inventory and security are different things. Then—often in the next sentence—they will indicate that they expect their inventory system to alert them to theft or diversion. It doesn't work that way. An inventory device, system, or program that makes no significant attempt to protect itself from tampering, spoofing, incapacitation, or other malicious attack, cannot be used to come to any meaningful conclusions about theft, diversion, tampering, espionage, or any other security concern.

Security is difficult enough when it is designed in from the beginning, when the various possible ways the adversaries can game the system are factored in. Effective security doesn't happen by accident when nobody is thinking about it, nor is it something that can be stuck on to an inventory system at the last minute in an *ad hoc* manner like some kind of band-aid.

It is also important to watch out for mission creep.[2] Systems that were originally intended for inventory only (no anti-spoofing measures and no nefarious adversary to counter) can quickly come to be viewed—quite incorrectly—as security systems.

Classic examples of dangerously confusing inventory and security in nuclear safeguards (and other security applications) include the use of radio frequency identification devices (RFIDs) or contact memory buttons (CMBs) for material control and accounting (MC&A), or the Global Positioning System (GPS) for cargo security. These technologies are inventory technologies, not security technologies, and can be easily spoofed.[2-7]

Countermeasures: (1) Don't use inventory technologies, devices, or systems for security, including RFIDs, CMBs, and GPS. (2) Understand the difference between inventory and security, and constantly be vigilant and warn people about mission creep. (3) If a given system must do both inventory and security, analyze it first for inventory efficacy, then start over and analyze it separately for security efficacy.

**Blunder 3**: Thinking that nuclear MC&A is an inventory function.

Comments: Nuclear MC&A—Material Control and Accounting (or Accountability)—superficially resembles an inventory function because it involves locating and counting nuclear assets. MC&A is, however, fundamentally a security function because it is meant to answer the question of whether there has been any nuclear theft, diversion, tampering, or espionage. Any meaningful MC&A system or program must make significant attempts to detect or deter spoofing by a nefarious adversary. Otherwise, we can have no confidence in what our (supposed) MC&A measures have to say about nuclear theft, diversion, tampering, or espionage.

We are sometimes asked, "What if my inventory system says something is missing. Shouldn't I investigate the possibility of theft or diversion?" Our response is that you should never ignore data, but there is a real danger in using inventory information for security purposes because inventory systems (by definition) make no attempt to counter a malicious adversary, and because this encourages mission creep and further confusion of inventory vs. security.

Countermeasures: (1) Constantly examine what countermeasures your MC&A system or program takes against spoofing, and whether they are sufficient to stand up to likely adversaries. (2) If the countermeasures are inadequate, draw no definitive conclusions about theft, diversion, tampering, or espionage until you can fix them. (3) Watch out for mission creep. (4) Never represent an MPC&A system or program as providing reliable security information when it does not. This does a true disservice to security.

**Blunder 4**: Having mindless faith in "Security in Depth" ("Layered Security" or "Defense in Depth").

Comments: Sometimes, multiple layers of security are necessary, but often they are a mistake, or at least have to be implemented with much more careful thinking about how the various layers work in conjunction with each other, and how they interfere with each other.[8] Too often, security managers think that multiple layers of bad security somehow will magically add up to good security. Having layered security is often correlated with over-confidence, and is frequently used as an excuse not to improve each individual layer of security, or deal with its vulnerabilities. For more

discussion of the potential problems with layered security and possible countermeasures, see reference 8.

Countermeasures: (1) Don't be complacent about layered security. (2) Think carefully about the various layers and how they interact, understand the role of each, and try to optimize each layer in its own right. (3) Don't deploy irrelevant layers.

**Blunder 5:** Not doing effective and periodic background checks on nuclear personnel as a means of mitigating the insider threat.

Comments: This is usually not a problem for domestic nuclear safeguards in the United States, but it is a problem internationally. For example, the International Atomic Energy Agency (IAEA), does no significant background checks on its inspectors.[7] This is the case even though they are allowed to go into nuclear facilities, are given partial diplomatic immunity, and the IAEA must rely on their findings to determine if a given country is fulfilling its nuclear obligations. Higher-level personnel at the IAEA who interpret the inspectors' findings, and laboratory technicians who work with radioactive sources at IAEA facilities are also not subject to significant background checks. This, despite the fact that the IAEA encourages member states to do background checks on their domestic nuclear personnel.[9]

Background checks are not an absolute panacea for the insider threat, but can nevertheless be an effective security measure. Not knowing if an inspector or other IAEA official has serious problems with character, loyalty, finances, drug or alcohol use, or is a potential terrorist or a wanted criminal is not only a risk to nuclear security and safety, but puts the IAEA's reputation at risk in a manner that could threaten future inspections, verification, and disarmament.

Countermeasures: Do periodic background checks on nuclear workers. The level of thoroughness and invasiveness should be commensurate with the risk of the insider threat.

**Blunder 6**: Believing that: (1) There are only a small number of security vulnerabilities and that they all can be neutralized; (2) Finding a vulnerability is bad news, or that it means automatically that somebody has been negligent; (3) A vulnerability assessment is some kind of test to be passed; and/or (4) The ideal outcome of a vulnerability assessment is to find zero vulnerabilities.

Comments: There are always a large number of vulnerabilities in any security device, system, or program, and most will never be discovered (by either the good guys or the bad guys). We believe this because we always find new vulnerabilities and attacks whenever we re-examine a physical security device, system, or program, and we usually find different vulnerabilities and attacks than other vulnerability assessors, and vice versa.

Finding a vulnerability is always good news because it means that something can potentially be done about it.

Countermeasures: (1) Try to view the discovery of vulnerabilities as good news, thus increasing the odds that the organization will be psychologically willing to implement countermeasures. (2) A vulnerability assessment that finds no vulnerabilities is useless and should be redone by more competent or motivated vulnerability assessors. (3) Recognize that the purpose of a vulnerability assessment is to improve security, not provide an arbitrary "certification" for a security device, system, or program. (It's not at all clear what it means to "pass" a vulnerability assessment.)

**Blunder 7**: Over confidence in design basis threat (DBT), or over confidence in other formalistic methods for analyzing security.

Comments: DBT—the idea that security should be designed to deal with the actual threat—

is common sense (despite the gibberish nomenclature). In our view, however, most DBT exercises are not particularly effective at identifying the security vulnerabilities most likely to be exploited by an adversary. This is because they are typically not done creatively enough, from the mindset of the adversary, or by personnel who are eager to find problems. The bottom line is that adversaries don't do DBT themselves, so if we are trying to predict what they might do, we need to use other techniques as well to "get inside their heads".

Many other formalistic tools for supposedly finding vulnerabilities (CARVER method, Delphi method, software vulnerability assessment tools, security audits, infrastructure or facility modeling, etc.) have value in our view, but are often primarily of use for deciding how to deploy security resources, rather than discovering vulnerabilities or predicting what the adversary might do.

Countermeasures: (1) Don't view DBT as a silver bullet, nor as some kind of "test" to be passed. (2) Use effective, independent, creative vulnerability assessors who want to find problems and suggest practical solutions. (3) Don't place undue faith in formalistic methods of doing vulnerability assessments because they will not typically find the most serious or obvious vulnerabilities.

**Blunder 8**: Failing to recognize that people are remarkably poor observers[10], they have serious perceptual and cognitive problems[10,11], flawed reasoning[12], and difficulty handling cognitive dissonance[8,13,14].

Comments: The old adage that "if you rarely see it, you often don't see it" can summarize a lot of what cognitive psychologists have learned over the past few decades about human perception. The fact is that people are very poor observers; they only see what they are mentally prepared to see.[10,11] This has very serious implications for security guards. Indeed, any security or safeguards program is in trouble if there aren't frequent "What if?" mental or walk-through exercises that encourage security personnel to envision possible attacks.

Misdirection and sleight-of-hand techniques of the sort that magicians employ can make accurate observations by security guards even more challenging.

Cognitive dissonance is the mental tension that arises when there is a conflict between what we want to believe—our security is good—and what is likely to be true—there are problems.[8,13] Cognitive dissonance itself is not the problem, but rather how we handle it. If handled poorly (as it often is), it can lead to *self-justification* (self-serving rationalization and excuse making), *paralysis* or *stagnation* (failure to confront serious problems or take necessary actions), *confirmation bias or motivated reasoning* (unduly dismissing ideas, arguments, evidence, or data that might call into question our current viewpoints, strong hopes, or past decisions). None of these things are good for security.

Countermeasures: (1) See reference 11 for potential countermeasures to perceptual blindness. (2) Some of the most effective countermeasures against cognitive dissonance are perspective, humility, skepticism, pragmatism, flexibility, a sense of humor (or at least not taking one's self overly seriously), and appointing a devil's advocate. It is also useful to bear in mind that it's always easier to fool yourself than anybody else.

**Blunder 9**: Automatically rejecting concerns, questions, criticisms, and feedback about security from any quarter, including from low-level security personnel. Attacking or retaliating against people who offer such feedback.

Comments: It's fairly common for organizations to ignore or even retaliate against insiders or outsiders (including vulnerability assessors) who raise concerns, questions, or criticisms about

security, or point out security vulnerabilities. This is incompatible with good security, and represents a missed opportunity to improve (or at least critically examine) security practices. Even questions and concerns that lack merit can lead to better understanding.

Countermeasures: (1) Security managers need to be eager to hear from anybody about security concerns and vulnerabilities, and take comments, questions, criticisms, and concerns seriously. (2) It is important to welcome, praise, and reward input, regardless of its ultimate usefulness. (3) Do not practice or tolerate any "shooting of the messenger".

**Blunder 10**: Confusing high-tech with high security.

Comments: In our experience, physical security devices, systems, and programs that rely on advanced technology are often easier to defeat than those that do not.[3] Misusing RFIDs, CMBs, and GPS for critical security applications is, in our view, often not just about confusing inventory with security, but also confusing advanced technology with effective security.[3]

Countermeasures: High-tech is not a silver bullet for security or safeguards. Bear in mind Bruce Schneier's philosophy that "If you think technology can solve your security problems, then you don't understand the problems and you don't understand the technology."[15] This doesn't mean advanced technology shouldn't be used for nuclear safeguards, but its effective use requires even more critical and careful thinking about security than when only low-tech is involved.

**Blunder 11**: Not having effective measures to deal with the insider threat, especially that motivated by disgruntlement.

Comments: Most organizations ignore or deal ineffectively with the insider threat. Many of the motivations for an employee to instigate an insider attack are difficult to neutralize—greed or radicalization for example. One common motivation, however, is disgruntlement, for which there are well-developed countermeasures. The Human Resource (HR) Department is one of the most important potential tools for mitigating employee disgruntlement, but in many organization, HR contributes to disgruntlement rather than working to resolve it.[16,17]

Countermeasures: (1) Treat everybody well, especially those leaving the organization. (2) Constrain HR tyranny and mistreatment of employees. (3) The organization must not tolerate bully bosses. (4) Have a fair and effective complaint resolution process for employees and contractors. Only the perceptions on the part of employees/contractors about the effectiveness and fairness matters. What senior management and HR think is irrelevant. (5) Senior managers should not point with pride to how little a complaint resolution process is used by employees and contractors. If a complaint resolution process is fair and effective, it will be used frequently. (6) Pay attention to whom in the organization is becoming disgruntled, and attempt to mitigate their disgruntlement.

**Blunder 12**: Treating employees, contractors, and visitors as if they are the enemies of security, not the allies. Letting security be perceived as the enemy of productivity.

Comments: This creates an "us vs. them" atmosphere, which is never conducive to good security, and encourages employees to scheme to overcome security rules. The fact is that—the insider threat not withstanding—employees, contractors, and visitors are our most powerful tools for implementing good security.

Countermeasures: (1) Don't let security be perceived as the enemy of employees or of productivity. (2) Avoid insulting, threatening, and boring security awareness training. (3) View and utilize employees, contractors, and visitors as powerful allies in the task of providing effective security. (4) Reward and recognize good security practice, don't just punish bad practice. (5)

Instead of the usual "security is everyone's responsibility" mindset and slogans, emphasize to general employees and visitors that "we need you to help with security and here is why, and here is what's in it for you."

**Blunder 13**: Inundating employees with too many, overly complicated, or constantly changing security rules, regulations, and policies. Not having anybody in the organization with the authority to unambiguously and fearlessly interpret, tweak, or push back on the security rules in particular cases. Imposing rules from above without doing a sanity check to see how they will impact regular employees. Having security rules that aren't well explained or justified to employees.

Comments: Bureaucratic, ineffective, vague, confusing, ill-conceived, or stupid security rules engender employee cynicism about security—which is very dangerous—in addition to wasting time and resources that could be better used to provide effective security. Security rules that appear arbitrary to employees may not be followed, and can cause cynicism about security even if they are. This may be more damaging than not having the rules in the first place.

Countermeasures: (1) Focus on the truly important security issues, and make them simple to understand and use. (2) Write security rules in plain English, not bureaucratese. (3) If the average employee cannot explain in 1-2 sentences why a security rule is in place and why it is important, either the rule needs to be removed, or it should be reviewed and better explained/motivated to employees. (4) Designate and empower security personnel to help interpret the rules for specific cases, and indemnify them against retaliation. (5) Before implementing new security rules or regulations, understand how they will impact productivity and the employees affected by them. Do this by talking directly with the affected employees. (6) Organizations and security managers should avoid the temptation to implement "knee jerk" changes in security rules and regulations after a serious security incident, or institute changes merely for punitive reasons.

**Blunder 14**: Confusing control with security.

Comments: Just because those in charge of security are delaying, hassling, threatening, intimidating, bullying, or micro-managing visitors and employees does not mean these actions automatically contribute to security. Doing these things often harms security (not to mention productivity, morale, employee retention, and the organization's reputation!). If security rules and practices make employees hate and distrust security, it won't be possible to have good security. Anytime security becomes the perceived enemy of productivity, security will suffer.

Countermeasures: (1) Any security rule, regulation, guideline, or policy should be reviewed to see if it is really more about control than about effective security. (2) The degree that a security rule or policy hassles or inconveniences employees is not a valid security metric. (3) Rules that only the good guys will follow (e.g., no cameras inside the facility, take your hat and sunglasses off in the bank) should be carefully examined.

**Blunder 15**: Thinking that encryption or data authentication provide absolute security.

Comments: Data authentication is closely related to data encryption. Both techniques actually add little security if there is not good physical security at the sending and receiving locations (which is usually the case), and/or if there is poor key control and personnel reliability. Data encryption and authentication have their uses, but they cannot guarantee the veracity of nuclear safeguards, monitoring, and surveillance data when the hardware or software is designed, constructed, provided, transported, controlled, or operated by untrustworthy personnel. There is no security if the sensor

or raw data can be tampered with (or counterfeited), or the secret key obtained, or the cipher broken through cryptoanalysis.

Countermeasures: Don't view data encryption and authentication as a panacea for security or verification. They are not silver bullets, nor a magic solution for reliable treaty verification (or for information barriers).

**Blunder 16**: Not having effective seal use protocols, or sufficient training for seal installers and inspectors.

Comments: Most or all seals (and tamper-evident enclosures) used for nuclear safeguards (domestic or international) are, in our view, unnecessarily easy to spoof.[1,4,7,18-20] A seal (or tag) is no better than its use protocol[18-20], which is how the seal is used. It includes the official and unofficial, formal and informal procedures for choosing, procuring, transporting, storing, securing, assigning, installing, inspecting, removing, and destroying seals. Other components of a seal use protocol include procedures for securely keeping track of seal serial numbers, and for inspecting the object or container onto which seals are applied. Training is another critical key element of an effective tamper detection.

Countermeasures: (1) Seal inspectors should have practical, hands-on experience with seals that have been attacked both in a subtle manner and not so subtle manner. They should understand the attack scenarios for the particular seal they are using and look for the most likely attack methods. They should be shown how to attack seals so they know what to look for. (2) Thorough visual and ideally tactile inspection of a seal is essential for reliable tamper detection, even for seals read with an automated reader. (3) Better seals are possible.[4,18,19]

**Blunder 17**: Not effectively dealing with high rates of security guard turnover.

Comments: The turnover rate for frontline security guards across a wide range of security organizations and applications typically ranges from 40% to 400% annually.[21] This represents an enormous economic problem, but also a serious security vulnerability.[21,22]

Countermeasures: Industrial/Organizational Psychologists have developed a number of proven tools for dealing with high employee turnover.[21,22] These tools, as well as other I/O psychology tools, have inexplicably not been applied to security or nuclear safeguards.

## CONCLUDING COMMENTS

By necessity, the common mistakes and countermeasures discussed here are general in nature. Security managers and practitioners interested in a more detailed discussion of some of these issues, particularly in the context of their own nuclear security and safeguards program, should feel free to contact the authors.

## ACKNOWLEDGEMENT AND DISCLAIMER

This work was performed under the auspices of the United States Department of Energy (DOE) under contract DE-AC02-06CH11357. The views expressed in this paper are those of the authors and should not necessarily be ascribed to Argonne National Laboratory or DOE.

## REFERENCES


1. Argonne National Laboratory, "Vulnerability Assessment Team", http://www.ne.anl.gov/capabilities/vat.

2. JS Warner and RG Johnston, "Why RFID Tags Offer Poor Security", *Proceedings of the 51st Annual INMM Meeting*, Baltimore, MD, July 11-15, 2010.

3. RG Johnston and JS Warner, "The Dr. Who Conundrum: Why Placing Too Much Faith in Technology Leads to Failure", *Security Management* **49**, 112-121 (2005).

4. JS Warner and RG Johnston, "Chirping Tag and Seal", *Proceedings of the 51st Annual INMM Meeting*, Baltimore, MD, July 11-15, 2010.

5. JS Warner and RG Johnston, "Contact Memory Buttons and Nuclear Safeguards", *Journal of Nuclear Materials Management* **37**, 11-15 (2009).

6. JS Warner and RG Johnston, "A Simple Demonstration that the Global Positioning System (GPS) is Vulnerable to Spoofing", *Journal of Security Administration* **25**, 19-28 (2002).

7. RG Johnston, et al., "Nuclear Safeguards and Security: We Can Do Better", *Proceedings of the 10th International Conference on Environmental Remediation and Radioactive Waste Management (ICEM'05)*, Glasgow, Scotland, Sept 4-8, 2005.

8. RG Johnston, "Lessons for Layering", *Security Management* **54**, 64-69, (2010).

9. IAEA, "Security in the Transport of Radioactive Material", *Nuclear Security Series No. 9, Implementation Guide*, 2008, http://www-pub.iaea.org/MTCD/publications/PDF/pub1348_web.pdf.

10. C Chabris and D Simons, *The Invisible Gorilla: And Other Ways Our Intuitions Deceive Us* (Crown, 2010).

11. RG Johnston, "Countermeasures for Perceptual Blindness", *Proceedings of the 51st Annual INMM Meeting*, Baltimore, MD, July 11-15, 2010.

12. C. Fine, *A Mind of Its Own: How Your Brain Distorts and Deceives* (Norton, 2006).

13. C Tavris and E Aronson, *Mistakes Were Made (But Not by Me): Why We Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts* (Mariner, 2008).

14. RG Johnston and JS Warner, "Security Theater in Future Arms Control Regimes", *Proceedings of the 51st Annual INMM Meeting*, Baltimore, MD, July 11-15, 2010.

15. B Schneier, *Secrets and Lies: Digital Security in a Networked World*, (Wiley, 2004), http://www.schneier.com/book-sandl-pref.html.

16. KH Hammonds, "Why We Hate HR", *Fast Company*, Issue 97, August 2005, http://www.fastcompany.com/magazine/97/open_hr.html?page=0%2C0.

17. KH Hammonds, "Writer Defends 'Why We Hate HR'", *Article, Business & Legal Reports*, 11/29/2005, http://compensation.blr.com/display.cfm/id/154876.

18. RG Johnston, "Tamper-Indicating Seals", *American Scientist* **94**, 515-523 (2005).

19. RG Johnston, "The 'Anti-Evidence' Approach to Tamper-Detection", *Packaging, Transport, Storage & Security of Radioactive Material* **16**, 135-143 (2005).

20. RG Johnston, "Tamper Detection for Safeguards and Treaty Monitoring: Fantasies, Realities, and Potentials", *Nonproliferation Review* **8**, 102-115 (2001).

21. E Bitzer, "Strategies for Cutting Turnover", *Security Management* **50**, 88-94 (2006), based on EG Bitzer and RG Johnston, "Turnkey Turnaround Solutions: Exploiting the Powerful Tools of I/O Psychology", *Los Alamos National Laboratory Report LAUR-05-1130*.

22. EG Bitzer, PY Chen, and RG Johnston, "Security in Organizations: Expanding the Frontiers of Industrial-Organizational Psychology", *International Review of Industrial and Organizational Psychology* **24**, 131-150 (2009).