Right Brain Sekurity

The Journal of Physical Security

Volume 9(2), 2016

(ISSN 2157-8443)

http://jps.rbsekurity.com

JPS

IN THIS ISSUE...

Table of Contents

Journal of Physical Security, Volume 9(2), 2016

Available at http://jps.rbsekurity.com

Editor's Comments

Welcome to volume 9, issue 2 of the *Journal of Physical Security* (JPS). In addition to the usual editor's rants and news about security that appear immediately below, this issue has papers about cargo security and the law, HR and security, combining safety and security, principals' views on school security, and an analysis of the productivity of the Department of Energy National Laboratories.

All papers are anonymously peer reviewed unless otherwise noted. We are very grateful indeed to the reviewers who contribute their time and expertise to advance our understanding of security without receiving recognition or compensation. This is the true sign of a professional!

Past issues of JPS are available at http://jps.rbsekurity.com, and you can also sign up there to be notified by email when a new issue becomes available.

JPS is hosted by Right Brain Sekurity (RBS) as a free public service. RBS is a small company devoted to physical security consulting, vulnerability assessments, and R&D. (http://rbsekurity.com)

As usual, the views expressed in these papers and the editor's comments are those of the author(s) and should not necessarily be ascribed to their home institution(s) or to Right Brain Sekurity.

*****

Safety Vs. Security

The third paper in this issue (Raphaël Duguay, "Enhancing Safety and Security Synergies to Improve Radioactive Source Security in Canada") is particularly intriguing because it discusses using safety personnel to conduct security inspections. I personally think this may be a mistake.

While safety and security personnel certainly must communicate and not get in each other's way, security usually suffers when it is too intertwined with safety. This is because the two activities are so different—one having a malicious adversary and the other not—and because in my experience, security suffers severely when it is viewed from the safety perspective and methodology, or done by safety personnel. [This being said, we certainly do not want to discourage safety personnel from speaking up about security problems they encounter or potential security improvements, or vice versa for security personnel regarding safety.]

Safety, lacking a deliberate adversary, is usually more comfortable and less complicated than security, and it will typically easily dominate security in a large organization, causing a

lack of critical focusing on security threats and vulnerabilities. Duguay, however, makes coherent arguments for the synergy of safety and security. What do you think?

*****

Your Security Stinks!

The SkunkLock, a crowdfunded new bicycle lock, has been developed by inventors in San Francisco. When cut into, the lock emits a noxious gas that smells so bad that it makes the burglar vomit. No word on the effect of quickly-freezing the lock to lower the vapor pressure. For more information, click here: [].

*****

Security Hinges

I've always been amazed at how often locked or sealed security doors or cabinets have the hinges on the outside. And how often security managers haven't noticed or don't think it's a problem. This is a really bad security practice, and totally unnecessary. Here are some web pages that discuss various cost-effective designs permitting the hinges to be in the interior and/or otherwise protected:

https://learningcenter.statefarm.com/residence/safety-1/door-hinges-and-home-security/
http://www.renovation-headquarters.com/hinges-security.html
http://www.sugatsune.com/hinges-door-accessories/
http://www.hardwaresource.com/hinges/door-hinges/invisible-hinges-and-soss-hinges/
https://www.doitbest.com/products/251887

*****

V2V

The federal government has been working on rules and standards for vehicle-to-vehicle communications (V2V). See []. This will allow cars to synchronize their movements and braking, and talk to traffic lights. The expected range for communications from a car is about 1,000 yards, including around corners. The proposed standards call for at least 128-bit NIST-approved encryption for security. To protect privacy, the V2V communications will be anonymous, with no identification information on the car or its owner. There is currently a 90-day open period for public comment. How much you want to bet that serious vulnerabilities and hacks will eventually be found?

*****

Automated Lip Reading

Researchers at Oxford University have developed an automated system that can watch silent videos of people speaking and read their lips. It reportedly substantially outperforms human lip readers. There are certainly counter-intelligence implications to this technology.

*****

Forensics on Forensics

Our legal system has convicted many thousands of people on the basis of junk science. A new study by the President's Council of Advisors on Science and Technology concluded that most forensic techniques have high error rates. Bite-mark analysis is completely bogus. Fingerprint analysis is wrong about 5% of the time. The analyses of firearm, ammunition, and hair are unreliable and not scientifically well-established. Even DNA analysis can have serious problems. See Alex Kozinski, "Rejecting Voodoo Science in the Courtroom".

*****

Flaws

Samsung had to recall and eventually cancel its new Note7 smart phone because the battery tends to burst into flames. (They are no longer allowed on planes.) As if that weren't bad enough, Samsung later had to recall 2.8 million Samsung washing machines after a number of them exploded during the spin cycle. Some people were injured and homes were significantly damaged. At least one lawsuit against Samsung alleges that the company knew about the problem for years yet took no action.

Problems with lithium-ion batteries are not completely surprising. The failure modes of these batteries are not well understood. (Quality control issues may have been involved.) What is more puzzling is the mechanical failure of the washing machines. The strength of materials for rotating machinery and the quality control issues needed in manufacturing have long been understood.

*****

The Dunning-Kruger Effect

David Dunning and Justin Kruger at Cornell University were awarded the 2001 satirical Ig Nobel Prize in Psychology for their discovery that incompetent people often don't know they are incompetent. Despite the "well duh!" nature of this discovery, the "Dunning-Kruger Effect", as it is now known, continues to be a serious matter for research and for practical management.

"The trouble with ignorance," says Dunning, "is that it feels so much like expertise." This is a major problem in security—especially the ignorance of vulnerabilities—and it also plagues politics, as the recent election cycle has amply demonstrated.

For more information on the Dunning-Kruger Effect, see [].

*****

Hacking the Beatles

For a really fun (and somewhat educational) account about teenagers defeating security to sneak into a Beatles concert in 1966, see Monica Hesse, "Their Goal: Meet the Beatles on Tour in 1966. Their Solution: Impersonate the Opening Act".

*****

Dr. Strangelove or Life Imitating Art

In the classic 1964 satirical movie, *Doctor Strangelove or How I Learned to Stop Worrying and Love the Bomb*, the Soviets turn out to have a nuclear doomsday machine which—to the consternation of the Americans—they haven't bothered to announce. This makes it of no value for deterrence. This scenario may not be as silly as it seems, or only relevant to past Cold War history. See articles on Deadhand and Perimeter.

*****

The Thing

Speaking of the Cold War, on August 4, 1945, the Soviets gave the U.S. Ambassador W. Averell Harriman a gift. It was a carved wooden copy of the Great Seal of the United States. Harriman promptly mounted the seal in a conference room inside the U.S. embassy in Moscow.

The seal turned out to be a passive listening device, now known as the "Thing" or the "Great Seal Bug". It was designed by Léon Theremin of theremin fame. The Thing was a sound-modulated resonant cavity requiring no batteries or electrical power. Microwaves were beamed externally by the Soviets from outside the embassy towards the device. The microwaves inductively coupled to the cavity, allowing sound in the conference room to be modulated into the scattered microwave signal so that eavesdropping was possible. The bug was eventually discovered by the Americans in 1951, mostly by accident.

For more information, see [].

Security lesson: don't accept gifts from adversaries, or at least don't put them in places that can compromise your security.

*****

The Crisis Theory of Security

Here's why it's important to continually discuss security—we want good ideas lying around: *"Only a crisis—actual or perceived—produces real change. When the crisis occurs, the actions that are taken depend on the ideas that are lying around."* -- Milton Friedman (1912-2006).

*****

How Not to Respond to Hackers

We are seeing played out in public an excellent example of how companies should NOT behave when told about potential vulnerabilities by vulnerability assessors or hackers. Hackers have claimed that medical products made by St. Jude Medical, Inc. have serious security vulnerabilities. See [].

St. Jude categorically denies there are any problems. I've seen this before. It is a foolish way to respond. Whether correct or not, a company's denial never seems believable even if the company is right (which it often isn't). It makes the company look uncaring. A knee-jerk denial just enrages the original and other hackers, and eggs them on to further exploits. Moreover, claiming that there are no economic incentives for attacking medical devices is disingenuous and not a satisfactory reason to ignore potential security problems in any medical device.

Whatever the facts, a public accusation of serious security vulnerabilities in its products is not the time for the manufacturer or vendor to go into cognitive dissonance mode, nor is it the time for Public Relations Amateur Hour. Hackers, the public, the news media, and the relevant security issues have to be handled with a certain degree of sophistication, intelligence, and understanding of the culture and psychology of hackers. The response should be planned in advance, before the hack! Better yet, figure out your own vulnerabilities before others do!

*****

Stop Clowning Around with Your Risk Assessment!

According to a poll conducted by Vox/Morning Consult, more Americans (42%) are afraid of clowns than a possible terrorist attack, a family member dying, climate change, or biological warfare. For more information, see: [].

*****

Ronald the Thug

The hamburger chain McDonald's announced that it's iconic mascot, the clown Ronald McDonald, would significantly reduce the number of public appearances due to "the current climate around [scary] clown sightings in communities." For more information, see: [].

*****

Real Risks

According to an AAA study, nearly 80% of all U.S. drivers admit to expressing significant anger, aggression, or road rage in the past year. About 4% of all drivers (8 million people) in the U.S. have intentionally rammed other cars or exited their vehicle to physically confront another driver out of anger. A total of 56% of all fatal auto accidents (nearly 22,000 deaths) are believed due to angry or aggressive driving. For more information, see: [].

According to the Washington Post, there were 33,092 deaths from opioids in 2015 in the U.S. The number of heroin deaths (12,989) surpassed the number of gun homicides for the first time in 2015. The dramatic increase in the use of prescription painkillers in recent years has contributed significantly to the problem.

*****

Sticky Risk

January 15 is the 97th anniversary of the Great Molasses Flood of 1919 that killed 21, injured 150 people, and destroyed numerous buildings in Boston. A giant storage tank of molasses ruptured, causing a tsunami of flowing molasses. In a new study, the physics of molasses flow was analyzed to better understand the disaster. See [].

The rupture of the tank was originally blamed on sabotage by anarchists. (Terrorism and violence by anarchists was a very real problem in the years 1890-1920, something that we often forget.) Now, however, the tank was believed to have ruptured due to a design flaw unrelated to a malicious attack.

*****

Food Tampering

Attacks from anarchists are not necessarily a thing of the past. A Greek anarchist group claimed to be planning to poison several soft drink and food products with chlorine and

hydrochloric acid. For more information, see [].

*****

Tampering with Your Junk

One of the perks of editing the *Journal of Physical Security* is that readers will occasionally make me aware of unusual security applications. I've studied tamper detection and tamper-indicating seals for many years but here is one application for seals I never envisioned: chastity devices.

Chastity devices for women are typically chastity belts, designed to prevent rape, sexual intercourse, and/or masturbation. The myth is that they were widely used during the Crusades—a knight would supposedly lock his lady into a chastity belt and then leave to search for the Holy Grail. In reality, chastity belts were probably not used until the 16th century, and then rarely. They are a much more modern phenomenon.

The prototypical female chastity belt apparently often uses a small brass padlock. This is not great security but it presumably introduces enough delay to cool heightened passions. Because of the more complex morphology, a male chastity device is a textbook example of when tamper-indicating seals make sense: when it is easier, cheaper, more practical, and sufficient to know that unauthorized access took place, rather than to try to prevent it with a barrier.

Some male chastity devices on the market (especially relatively soft plastic and silicone ones) turn out to come with cheap, thin, light-weight, serial-numbered, one-time-use plastic seals. The partner of the wearer can simply check if the chastity device is intact, the seal still in place, and the serial number is correct. This demonstrates whether unauthorized sex, masturbation, or perhaps (depending on the design) if full erection took place.

Can't say I'm real enthusiastic about doing vulnerability assessment consulting or cargo security training on this particular security application, thank you very much, but it *is* an interesting use for seals.

*****

Social Media Versus Terrorist Scum

The big social media companies (Facebook, Twitter, YouTube, Microsoft) are teaming up to fight terrorism. The companies will create a shared database with hashes of terrorists' photos and images. This should allow them to more easily and quickly remove terrorist content that violates their policies. The database will not contain any personally identifiable user information. For more information, see [].

*****

Low-Tech Money Counterfeiting

Peter Holley in the *Washington Post* had an interesting article about the money counterfeiting "industry" in Peru. Peru is believed responsible for manufacturing about 60% of the world's counterfeit U.S. currency.

The Peruvian counterfeiters are artisans, making effective counterfeit notes with relatively low-tech methods. This is a consistent theme in counterfeiting, whether we are talking money, counterfeit products, fake documents, or spoofing attacks on tags and seals. The bad guys don't usually have to counterfeit at all, just mimic. While counterfeiting is often easier than people think, mimicking—where you approximately replicate certain attributes—is much easier and cheaper.

For more information about the Peru counterfeiting and a recent seizure of fake bills, see: [].

*****

More Money Fakery

The government of India claimed its new, high-tech 500 and 2000 Rupee notes could not be counterfeited, but fake notes quickly appeared all over India. The fakes are mostly made using relatively low-tech methods. For more information, see: [].

*****

Counterfeit Drugs

Drugs obtained from Prince's Paisley Park estate by authorities were counterfeit pills that illegally contained fentanyl. That is a powerful painkiller that an autopsy report said caused his death. For more information, see: [].

According to the World Health Organization, perhaps as many as a million people die every year worldwide from counterfeit drugs.

*****

Between the Sheets

The world of textiles has been rocked by a major problem with counterfeit Egyptian cotton. Egyptian cotton is famous for its quality, durability, and softness. Fake Egyptian cotton, while it is usually real cotton, is inferior and less expensive than the real thing.

Target, Walmart, and other companies have been burned by fake Egyptian cotton. It is not easy for consumers to identify the fake cotton, and even experts often have to run tests. For more information, see [].

*****

Counterfeit North Koreans

China, the nation that leads the world in counterfeit products, is now reportedly rolling out fake North Koreans. Private academies in China tutor ethnic Koreans who are Chinese citizens on how to pass as North Korean defectors. The fake defectors do this to in order to try to get asylum in Europe, and receive government assistance and free medical care.

*****

Security Logic, Metrics, and Minimizing Risk

Two articles on novel ways to think about security:

RG Johnston, "Common Reasoning Errors in Security", http://www.asiapacificsecuritymagazine.com/common-reasoning-errors-in-security/

RG Johnston, "Some Unconventional Security Metrics", http://www.asiapacificsecuritymagazine.com/some-unconventional-security-metrics/

The second article discusses "Marginal Analysis", a technique for Risk Minimization that is often thought of as more theoretical than practical. This article argues it has multiple real-world merits for promoting better, more proactive security, especially for complex security programs.

*****

Litmus Test

Here is a simple test to determine, with some accuracy in my experience, whether an organization has a poor Security Culture and thus poor security when you aren't a vulnerability assessor or can't examine the security in detail. The answer to several or all of the following questions will be yes:

1. Does the organization depend strongly on "Security by Obscurity", i.e., keeping secrets? Somewhat counter-intuitively, security is better when it is transparent because people and organizations can't keep secrets and because transparency allows for review, analysis, questioning, criticism, accountability, understanding, and buy-in.

2. Is the concept of "layered security" ("defense in depth") highly embraced? Organizations that rely too heavily on layered security, and mostly think about security in those terms

usually have poor security. It is not that layered security is inherently a bad idea. Rather, layered security often becomes an excuse to avoid thinking critically about security, optimizing each layer, and conducting essential vulnerability assessments. Too often, the various layers do not actually back each other up, e.g., fences and badges do little to counter insiders. Sometimes, the layers have a common mode of failure or even get in each other's way. Layered security also tends to engender the attitude that, "I don't recognize that guy walking off with our organization's critical assets, but I am sure it will be ok because we have many layers."

3. Does the organization do little or nothing in the way of effective vulnerability assessments, or confuse them with threat assessments, asset identification, feature analysis, security surveys, compliance auditing, "Red Teaming", penetration testing, design basis threat, fault/event trees, safety analysis, reliability/performance testing, or overall risk management? (These things are all useful but do not identify vulnerabilities to nearly the same extent as a true vulnerability assessment.)

4. Does the "Mr. Spock Security Maxim" apply?: "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." In a poor Security Culture, questioners and critics are attacked, and aspersions are cast on their motivations.

5. Does "Feynman's Security Maxim" apply?: "An organization will not have good security when it fears and despises loyal vulnerability assessors and others who raise concerns, point out vulnerabilities, or suggest security changes more than malicious adversaries."

6. Does Tacitus' observation apply?: "To show resentment at a reproach is to acknowledge that one may have deserved it." -- Tacitus (55-117 AD)

7. Is there arrogance or confidence in the security? With security, all confidence is over-confidence. (Public bluffing about how good the security is, is not an effective long-term security strategy. And the organization tends to come to believe its own PR.)

*****

Litmus Test for HR Incompetence

The second paper in this issue is a Viewpoint Paper that discusses HR charlatanism and HR's often negative impact on an organization's security. The following are 4 common HR practices that many management experts now think are poorly-conceived relics from the past that harm employee morale and productivity. They may also negatively impact security.

1. Formal Progressive Discipline Programs. This kind of approach may be appropriate for dealing with children and dogs, but makes no sense for adults that you want to be loyal to your organization.

2. An Employee's Current Manager Controls Internal Transfers and Promotions. In healthy companies, employees are not thwarted in their career goals or in opportunities to advance.

3. Formal Performance Management. Forcing employees to be accountable on a daily, weekly, monthly, or yearly basis to an arbitrary set of tasks and goals belongs in the Dark Ages. No real job breaks down into a series of rigid, tiny components, nor is micro-management usually a good idea, especially if you want to encourage star performers.

4. Nurturing Bully Bosses. HR Departments that ignore or even protect/encourage bully bosses substantially increase the insider risk. This also contributes to poor employee morale, lower long-term performance, increased medical costs, high employee turnover rates, and a bad reputation for the organization.

*****

Self-Fulfilling Prophecy

A Trump supporter in Iowa was arrested on a first-degree charge of election misconduct when she voted a second time for Trump. She indicated she feared her first vote wouldn't count because of election fraud, so she decided to cast a second vote. "The polls are rigged" she was quoted as saying**.** For more information, see: [].

*****

Profiles in Wackiness

Kazem Finjan, Iraq's Transport Minister, told reporters in September that his country's new airport would be built on the site of a Sumerian spaceport built by aliens 7,000 years ago. Seems like an appropriate location. For more information, see: [].

*****

Strongmen and Diplomacy

Gideon Rachman had an interesting article in the *Financial Times* about the global rise of the strongman leader, for example, Vladimir Putin (Russia), Rodrigo Duterte (Philippines), Xi Jinping (China), Recep Tayyip Erdogan (Turkey), Viktor Orban (Hungary), Shinzo Abe (Japan), Narendra Modi (India), and now Donald Trump.

According to Rachman, "Strongmen bring a distinct style to international diplomacy. They tend to want to sort things out man-to-man, rather than relying on institutions or international law." This tends to result in erratic, unstable, and unsustainable agreements.

*****

This Also Applies to Security, Vulnerabilities, and Risk Assessments

Emma Roller in an essay in the *NY Times*:

"The strongest bias in American politics is not a liberal bias or a conservative bias; it is a confirmation bias, or the urge to believe only things that confirm what you already believe to be true. Not only do we tend to seek out and remember information that reaffirms what we already believe, but there is also a "backfire effect," which sees people doubling down on their beliefs after being presented with evidence that contradicts them. So, where do we go from here? There's no simple answer, but the only way people will start rejecting falsehoods being fed to them is by confronting uncomfortable truths."

For more information, see: [].

*****

Befriending Censorship

Facebook is reportedly developing software that would permit localized censorship of its content, perhaps as a way to be allowed back into China. The project is controversial inside Facebook. For more information, see [].

*****

Women and Security

Empirical research shows that the best predictor for the stability, peacefulness, and security of a nation is not its wealth, degree of democracy, or ethic/religious attributes, but rather how well women are treated in that country. For more information, see: [].

*****

The Real Threat

The real threat to public security isn't Islamic terrorists, it's males. Melissa Batchelor Warnke in the *Los Angeles Times* points out that in the United States, 98% of those who commit mass shootings are male. 98% of police officers who have shot and killed civilians are male (out of proportion to their numbers), and 80% of those arrested for all violent crimes are male. Men are nearly 50 times more likely to commit murder than women.

*****

Ban-the-Box Laws & Unintended Consequences

New research and analysis suggests that "ban-the-box" laws don't help ex-criminal-offenders and may actually worsen racial bias in hiring. "Ban the box" laws prohibit public and sometimes private employers from inquiring about an applicant's criminal history until late in the hiring process. (The "box" refers to the box that job applicants often are asked to check on their job application forms as to whether they have ever been convicted of a crime.) The intent with these laws is to make it easier for ex-offenders to get a second chance, but this appears to be a matter of unintended consequences. For a good discussion, see [].

*****

Top Secret

Each year, the Panatone Color Institute gathers color experts in—I kid you not—a secret European location to decide the official color for the year. (Some secrets may not really be worth the effort to protect!)

The official Pantone color for 2017 is Greenery. This color is "a refreshing and revitalizing shade ... symbolic of new beginnings". "Greenery is a fresh and zesty yellow-green shade that evokes the first days of spring when nature's greens revive, restore and renew. Illustrative of flourishing foliage and the lushness of the great outdoors, the fortifying attributes of Greenery signals consumers to take a deep breath, oxygenate and reinvigorate." For more color commentary, see [].

*****

I Think That I Shall Never See... 3 Trillion Trees

Speaking of greenery... a new study by researchers at Yale University shows there are about 3 trillion trees on the planet Earth, much more than originally thought.

*****

-- Roger Johnston
Oswego, Illinois
December, 2016

Viewpoint Paper

When Physical Security Fails: Minimizing Legal Risk and Financial Loss in the Transportation of Goods

Brent Wm. Primus, J.D.

Primus Law Office, P.A.
331 Second Avenue South
Suite 710, Minneapolis, MN 55401-2239

Overview

When physical security fails, what is your "Plan B"?

One element of physical security is the protection of the goods and commodities belonging to a company or organization. This could include measures ranging from perimeter fencing to the screening of persons seeking employment, as well as countless others. Typically, these functions would be performed by the employees of the company or by the company contracting with firms specializing in providing such security.

However, when the property is to be transported from one location to another, the physical security of an organization's property must typically be entirely entrusted to others. These entities will actually take possession and move the property with virtually no visibility or operational control by the owner of the property.

Within the U.S. legal system, these entities are known as motor carriers and rail carriers when moving goods over land, that is, trucking companies and railroads. When moving goods over water, the carriers could be ocean carriers or inland water carriers. When moving goods through the air, they are known as air carriers or airlines.

There are also entities known as intermediaries which can include transportation property brokers, surface freight forwarders, ocean freight forwarders, non-vessel operating common carriers (NVOCCs), and indirect air freight forwarders. These entities are known as "intermediaries" because their business model is to act as a "middleman" to arrange for the transportation of property by actual carriers on behalf of their customers who are the owners of the property.

And while on the topic of terminology, in this article, the customers of these providers, both carriers and intermediaries, will be referred to as "shippers". It should be noted that in common parlance the term "shipper" is often used to describe the carrier as well as the customer.

Most shipments of property arrive at the destination reasonably on time and relatively intact. However, when there has been a breach of the security or safety of the products, resulting in the products being damaged, it is incumbent upon the property owners to successfully pursue a claim for loss or damage to the property in order to minimize the financial loss caused by the damage to the property. The goal of this article is to provide security professionals with an introduction to the basic legal principles relating to claims for cargo loss and damage.

The late William J. Augello, co-author of *Freight Claims in Plain English*, had a passion about this topic as few others have. I believe that there are at least two reasons why Bill felt so strongly about the importance of understanding claims.

The first reason is financial. Unrecovered claims have a direct impact upon the bottom line of a company—and the tougher the economic times and thinner the margins the greater the impact. As depicted in the following chart, if your company operates at a 5 percent profit margin, to recoup the net revenues that would be lost by failing to recover a $1,000 cargo claim, it would have to generate $20,000 in sales!

Financial impact of unrecovered cargo claims

If you operate at net profit of	A claim of $50	$100	$200	$300	$400	$500	$1,000
	equals sales of						
2%	$2,500	$5,000	$10,000	$15,000	$20,000	$25,000	$50,000
3%	1,667	3,333	6,667	10,000	13,333	16,667	33,383
4%	1,250	2,500	5,000	7,500	10,000	12,500	25,000
5%	1,000	2,000	4,000	6,000	8,000	10,000	20,000
6%	883	1,667	3,333	5,000	6,667	8,333	16,667

Source: transportlawtexts, inc.

Second, Bill believed that this knowledge is vital for shippers because they're on their own when it comes to claims. For carriers, whose core business is transportation, the processing of claims is an integral part of their business, and all but the smallest of carriers are quite knowledgeable and very competent when it comes to defending against claims. For most retailers, manufacturers, and distributors, the transportation function is an unwanted headache—and claims represent a migraine.

Basic legal principles

The starting point in understanding cargo claims is to understand that a claim is based upon a breach of contract by the carrier, not whether the carrier was negligent. This arises out of the fact that the essence of a transportation contract is that the carrier agrees to move a piece of cargo from point A to point B. In return, the shipper agrees to pay the carrier.

Implicit in this arrangement is that the cargo will indeed arrive at destination…and in an undamaged condition. When the cargo is lost or damaged, the basic contract for carriage has been breached, giving rise to the shipper's claim.

The contract for carriage can either be an individually negotiated contract between the shipper and the carrier; or, if none, the bill of lading, waybill, ocean bill, or other document issued by the carrier. These documents will typically incorporate by reference the terms of the carrier's tariff or service guide or otherwise titled terms and conditions. The term "incorporate by reference" simply means that the contents of one document are incorporated into the document at hand. An example would be a bill of lading referring to the carrier's tariff, i.e., the other document.

Generally speaking, the claimant has the initial burden of proving its claim. The claimant must prove good condition at origin, damaged condition at destination, and the amount of its damages. After establishing these three elements, the burden of defense shifts to the carrier.

Different rules apply depending upon mode

Another very basic principle that must be kept in mind when dealing with a claim is that different legal principles and rules will apply depending upon the mode of

transportation. Motor, rail, domestic water, international ocean, domestic air, or international air all have different time limits for filing claims and different deadlines for initiating lawsuits if a claim is denied.

At one time the majority of carriers only operated in one particular mode. Now, many entities operate in more than one mode. For instance, UPS is licensed as a motor carrier, an air carrier, and a non-vessel operating common carrier (NVOCC).

Accordingly, an important initial step in analyzing any claim is to determine which mode the carrier was operating in at the time of the loss and thus which liability regime would apply. This can be very challenging for international movements involving multiple carriers and various modes.

Basics of motor & rail carrier liability

The starting point for rail and motor carriers are two federal statutes--49 U.S.C. § 11706 for rail and 49 U.S.C. § 14706 for motor—that are colloquially known as the Carmack Amendment. Under both of these statutes, the liability imposed is "for the actual loss or injury to the property." However, carriers are allowed to limit their liability in exchange for a lower rate, and most do so.

Carmack also sets minimum time standards for filing claims (nine months from the date of delivery) and for initiating lawsuits (two years from the date the claim is denied). It should be noted that the federal statutes do not themselves set these limits, but only prescribe the minimum. The significance of this is that if there is no tariff—as is often the case with small trucking companies—then there is no time limit to file a claim nor a two-year limitation on filing a lawsuit.

It should also be noted that Carmack only applies if the carrier is providing a regulated service subject to federal jurisdiction. When transporting an exempt commodity, like livestock, or operating in intrastate commerce (totally within one state), Carmack does not apply. For such shipments, the carrier could have tariff rules providing for shorter time limits than the minimum required by the Carmack Amendment.

The essence of Carmack is that carriers are considered to be virtual insurers and are strictly liable for cargo claims. There are, however, five recognized exceptions or defenses: (1) an act of God, (2) an act of the public enemy, (3) an act of a public authority, (4) an act of the

shipper, or (5) an inherent vice of the product. And, even though one or more of these factors might be present, the carrier must also show that it was free of negligence.

At least that is what the U.S. Supreme Court stated in a 1964 decision[i]. However, it should be noted that the motor carrier community has recently revised a widely used document known as the Uniform Bill of Lading in an attempt to reverse this holding by the U.S. Supreme Court by adding language to the Uniform Bill of Lading asserting that the claimant must prove that the carrier was negligent.[ii]

Ocean cargo liability

Ocean shipments to and from the U.S. are by and large governed by the Carriage of Goods by Sea Act (COGSA). This, in turn, is based upon an international treaty known as the Hague Rules. Under COGSA, an ocean carrier has 17 defenses; however, as with Carmack, even when the facts establish such a defense the carrier must also show that its negligence did not contribute to the loss.

For ocean shipments, the deadline to give notice of a claim is three days from delivery, much shorter than the nine months allowed under Carmack. Similarly the timeline to file suit is one year from the date of delivery—as opposed to two years from the date of declination of a claim under Carmack.

Originally COGSA was understood to apply tackle-to-tackle, meaning from the time that loading the shipment began to the completion of unloading the shipment. However, over time, the ocean carriers have been allowed to extend the COGSA liability regime to its subcontractors. A 2010 decision of the United States Supreme Court held that an ocean carrier can indeed extend COGSA to the inland portion of the movement by a motor or rail carrier through its bill of lading or other contracts.[iii]

Another significant difference between COGSA and Carmack is that whereas Carmack imposes liability for the actual loss, the liability of an ocean carrier under COGSA is limited to $500 per package or customary shipping unit. It's for this reason that most shippers obtain shippers' interest cargo insurance for ocean movements rather than to rely on the liability of the carrier as is the general practice with motor carriers.

At some point in the future, COGSA will be superseded. In December 2008, the General Assembly of the United Nations adopted the final draft of the United Nations Convention of

Contracts for the International Carriage of Goods Wholly or Partly by Sea colloquially known as "the Rotterdam Rules." It is generally felt that the change will be of benefit to shippers, but the Rotterdam Rules will not go into effect until ratified by 25 countries, including the U.S. As of December 2016, only three countries—Spain, Togo, and Republic of the Congo-—have ratified the treaty.

Air cargo liability

Different rules apply for domestic air shipments or international air shipments. For domestic shipments, the air carrier's tariff sets the time limits and limits of liability. These limits can be quite short—seven days or even less. The limit of liability can also be quite low—$0.50 a pound.

For international shipments, the Montreal Convention of 1999, an international treaty, sets the time limits and limits of liability. A claim must be filed within 14 days of delivery for damage and within 21 days for delay.

While the Convention does not provide a time limit for claims for non-delivery, the airlines typically set a limit of 120 days from the issuance of the air bill for notice of non-delivery. The statute of limitations for filing a lawsuit is two years; and under the Convention the current limit of liability is 19 Standard Drawing Rights (SDRs) per kilo, which translates to approximately $12.95 per pound.

Claims & claims filing

Whatever the mode, the first step to recover a loss and damage claim is the filing of a claim. The purpose of the claim is to put the carrier on notice of the facts relating to the damage or loss so that the carrier may investigate the claim and make a decision whether to pay it, decline it, or offer a compromise amount in settlement.

Although not at all in the nature of a lawsuit, the timely filing of a claim is a prerequisite for any later litigation. If a claim with a motor carrier is not filed within nine months, the claim is extinguished.

The mechanics of claim filing are far beyond the scope of this article. Suffice it to say that if not done correctly or within the applicable time limits, the result can be an unrecoverable claim. When there is no individually negotiated contract in place between

the shipper and the carrier, the claimant must look at the carrier's tariff provisions very carefully to see if that carrier has specific filing requirements.

Also, it is very important that the claim be filed with the transportation carrier, as opposed to the insurance carrier. A claim filed with the insurance carrier, rather than the carrier providing the transportation service, is not considered a duly filed claim for purposes of meeting the claim filing time limit.

Shippers and intermediaries

This article is focused on the liability of carriers, however, shippers can also be liable for cargo damage if the shipper caused the damage. An example of this would be a shipment by a motor carrier when a poorly packaged liquid breaks open and stains or otherwise damages other cargo on the truck. When the shipper is responsible for damage to other cargo, the carrier would ordinarily pay the other's party damage and then seek reimbursement from the shipper.

With respect to transportation intermediaries, as a general principle, they are not liable for cargo damage. However, intermediaries can be liable for cargo damage if they hold themselves out as a carrier, assume liability by contract, or the damage is caused by the intermediary's breach of contract. It must also be kept in mind that some entities that shippers think of as intermediaries may, in a legal sense, actually be carriers—for example, surface freight forwarders or so-called indirect air carriers.

Cargo insurance & cargo liability insurance

I would be remiss in this article if I did not touch upon insurance. One very important distinction is that between "cargo insurance" and "cargo liability insurance."

The carrier purchases cargo liability insurance which only pays to the extent that the carrier is liable. Thus, while a high-value product such as a mainframe computer may have been totally destroyed in transit, if the carrier had in place a valid tariff limit of $0.10 per pound for used equipment, the dollar amount of the carrier's liability would be negligible compared to the value of the product.

Accordingly, shippers must always keep in mind the option of purchasing shippers' interest cargo insurance to cover such situations. A shippers' interest cargo insurance policy is

not based upon fault. Thus, a carrier's limit of liability, whether it be a motor carrier's private tariff rule or an international treaty, is irrelevant. However, as with any insurance policy, it will have its own exclusions and deductions that must be carefully scrutinized by shippers to ensure that their freight is indeed insured.

Contracting away from carrier liability limits

I would be equally remiss in this article if I did not mention the role of an individually negotiated contract between a shipper-customer and its carrier or intermediary providers. The primary function of an individually negotiated contract, in addition to the documentation of the rates to be charged, is the negotiation of business terms and conditions which are more favorable to the customer than the standard terms and conditions of a carrier which would be in effect in the absence of an individually negotiated contract.

For instance, an individually negotiated contract could establish a higher limit of liability than typically offered by the carrier, e.g., $25.00 per pound rather than $5.00 per pound. Also, in an individually negotiated contract, an agreement could be reached whereby an entity such as a transportation broker would agree by contract to be liable for loss and damage to cargo even though it would not otherwise be so. To state the obvious, the degree to which a shipper-customer can negotiate beneficial terms is directly related to the amount of business that the customer will be giving to the provider.

Knowledge Is Still Power

The phrase "*scientia potentia est*" is commonly attributed to Francis Bacon, having stated it more than 400 years ago.[iv] Although we are now in the 21st Century, the phrase is just as true now as then.

And by the way, once a loss occurs it is too late to create a "Plan B".

References

i. Missouri Pacific R. Co. v. Elmore & Stahl, 337 U.S. 134 (1964), rehearing denied, 377 U.S. 948

ii. See *NMFTA Drops a Bombshell --- A New Uniform Bill of Lading!*, Parcel Counsel, *Parcel* magazine, September-October, 2016, by Brent Wm. Primus, J.D.

iii. Kawasaki Kisen Kaisha Ltd. v. Regal-Beloit Corp., 130 S.Ct. 2433, 561 U.S. 89, 177 L.ed.2d 424, 78 U.S.L.W. 4651 (2010)

iv. More on "*scientia potentia est*" may be found in a fascinating Wikipedia article: https://en.wikipedia.org/wiki/Scientia_potentia_est

About the Author

Brent Wm. Primus, J.D. is the CEO of Primus Law Office, P.A. and the Senior Editor of transportlawtexts, inc. He is the author of *Motor Carrier Contracts Annotated* and co-author of *U.S. Domestic Terms of Sale and Incoterms 2010*. He served as the *Editor of Freight Claims in Plain English*, 4th Edition. Brent can be reached at brent@primuslawoffice.com.

Viewpoint Paper

Is HR Helping or Hurting Your Security?*

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity (http://rbsekurity.com)

In theory, the Human Resources (HR) Department is one of the most powerful tools an organization has for improving security and reducing insider threat (both deliberate and inadvertent). In many organizations, however, HR makes security worse. This tends to be especially true in large organizations.

Rather than working to improve security, far too often HR becomes the enemy of employees—the much hated and feared tyrannical Rule-Maker, the condescending Insulter of Intelligence, and the Squasher of Productivity, as well as the Secret Police, Judge, Jury, and Executioner.

The common failure of HR to address employee disgruntlement is a particularly serious missed security opportunity that has important implications for the insider threat. There are a number of motivations for deliberate inside attacks. These include: greed; ideology, political activism, and radicalization; terrorism; coercion/blackmail; desire for excitement; the phenomenon of a self-identified Cassandra; disgruntlement; and (maybe) mental illness. Of all of these, disgruntlement is often the most straightforward to mitigate. But all too often, HR takes troubled or unhappy employees and turns them into enraged, disgruntled employees bent on retaliation.

It is particularly dangerous to have—as is often the case—phony or missing grievance and complaint processes. The same is true for missing, bogus, or ineffective employee

*This paper was not peer reviewed.

assistance programs to help employees with, for example, addiction problems, financial difficulties, mental health issues, and domestic strife including domestic violence. The best metric for success for these grievance and employee assistance programs is that they get used a lot. HR and senior executives, however, often brag about how little these programs get used in their organization, as if this were a sign of strength! Instead, it is a sign that employees recognize the programs to be useless, fraudulent, and/or dangerous to use.

All too often, HR fails to encourage effective, proactive methods for improving employee morale and reducing employee turnover. The latter is a particularly serious economic and security problem when there is a high turnover rate for security officers or IT specialists.

Moreover, HR often fails to watch intelligently for common precursors to insider attacks. These include **changes** in an employee's:

- hygiene
- performance
- rule compliance
- use of drugs or alcohol
- signs of aggression or hostility
- being late for work or a no show
- not getting along with co-workers

(The challenge, of course, is that while many insider attackers will show these precursors well before an attack, the vast majority of employees who exhibit such changes will never attack.)

Too often, HR fails to intelligently oversee appropriate and proportional disciplinary action. HR typically loves scapegoating after security incidents. HR often dangerously mistreats contractors, retirees, and terminated employees. And, of course, HR misogyny and racism has a long history, as does making inept and uninspired hiring choices [1].

*****

Certainly HR charlatanism is nothing new. I was recently reminded of this by looking at some management textbooks from 100 years ago. In particular, I read some of the popular HR guides to "reading" and evaluating character based on an individual's physical attributes. (See, for example, references [2] and [3].)

This kind of pseudo-scientific nonsense is called "physiognomy". It involves attempting to assess a person's character, personality, or optimal work assignment based on his/her outer appearance, especially of the face or head. Physiognomy has a very long history, going back thousands of years. While social scientists in the late 19th and early 20th century increasingly recognized physiognomy as quackery and it fell somewhat out of favor, the "theory" continued to be taught in college and used to some extent by businesses and HR ("Personnel") Departments more than two decades into the 20th century.

Judging character and temperament using physical attributes was typically presented as very "scientific" and objective [2,3], but it was neither [4,5]. And it was often racist and sexist.

Some samples of the "scientific" facts taught by one prominent 20th century proponent of physiognomy for HR purposes, Katherine M.H. Blackford, offer a flavor of this "methodology".

According to Blackford, indications of impulsiveness in a potential employee could be spotted if the person had "blonde coloring;…small, round retreating chin; small size;…short head; short, smooth fingers, with tapering tips; a keen, alert, intense expression" and if "….He walks with a quick step, sometimes almost jerky."[2]

Generally [3], "Thinkers" have a triangular face, and "Doers" (such as laborers) have a square face. "Mental-Motive" types, a combination of the two, have a squarish forehead and a triangular lower face. "Organizers" have a somewhat roundish face. Interestingly, Blackford did not require quantitative measurements in order to judge someone based on their face; qualitative assessments by the observer were adequate.

Blackford had particular opinions about "fat men". She believed fat men tend to be calm. She also maintained that, "Mentally, the average fat man is not very keen on abstruse subjects, does not care much for theories, doesn't delve very deeply into scientific and philosophic study, and is not much given to 'isms'. Wherever you find a crowd of radicals and fanatics together, you will almost always find a crowd of lean and hungry looking people." [3 page 21]. (The idea that young and hungry people might tend to be the social agitators, rather than well-fed fat and older people, especially 100 years ago, would not seem to require physiognomy!)

Interestingly, even Blackford appears to have had some concept of insider threat: "When employers select men unfitted for their tasks, assign them to work in environments where they are handicapped from the start, and associate them together and with executives in combinations witch are inherently inharmonious, it is inevitable that trouble should follow."[2]

*****

Nowadays, HR charlatanism and the use of pseudo-scientific nonsense is unfortunately not a relic of the past. Polygraphs (an "invention" from the same era as the Blackford textbooks) are an example of pseudo-scientific nonsense that is still alive and well in many corporations and government agencies. Other common HR charlatanism includes the arbitrary rejection of (or sometimes failure to properly reject) employment candidates with minor (or even major) criminal and drug histories. Questionable policies and hiring decisions based on (often easily spoofed [6,7]) drug testing is another common area of HR charlatanism, as is sloppy background checks and the frequent failure to motivate good security and safety practices. There are many other examples of dangerous and foolish HR policies and practices that harm security.[8]

Traditionally, if HR Departments are evaluated at all, they are usually evaluated from a business, management, or compensation/benefits perspective. It is a huge vulnerability, however, not to periodically evaluate HR from a security standpoint, focusing especially on Security Culture and insider threat mitigation. This is probably best done by external Vulnerability Assessors who are less susceptible to retaliation and "shooting the messenger" than internal personnel. External assessors also offer a more objective view and tend to be less constrained by the organization's politics and cultural problems.

When HR fails to support good security—or is even actively undermines it—security managers can help the organization by pushing for a security evaluation of HR policies and practices, or at least warning HR, managers, and senior executives that HR is creating serious security vulnerabilities. Given that doing these things may put your own job at risk, it is often not an easy thing to do. A safer alternative may be to try to provide some of the security countermeasures yourself that HR is failing to provide. For example, as a security manager, you (and subordinates) can watch for the precursors to insider attacks if you have good formal and informal relations/communications with employees, contractors, supervisors, and managers.

You might even be able to partially mitigate disgruntlement. For example, you could exploit (or encourage others to exploit) the so-called 80% Rule: when an employee is disgruntled, if someone in the organization with even a little authority will simply listen to, validate, and empathize with the employee, approximately 80% of the time the employee will feel significantly better about the problem, himself/herself, and the organization as a whole. Remarkably, it isn't even necessary to agree with the employee about their complaint(s), or fix whatever is bugging him or her—though, when possible, a sincere attempt to fix the problem can go a long ways towards eliminating the disgruntlement.

When HR isn't doing what they need to do to reduce security vulnerabilities (especially in regards to engendering a healthy Security Culture and mitigating employee disgruntlement), perhaps it is up to you as a security manager to try to compensate for HR's arrogance, ignorance, recklessness, and incompetence when it comes to security.

Notes and References

1. Paul Goodman (1911-1972) famously noted that "Few great men would have got past Personnel."

2. Katherine M. H. Blackford and Arthur Newcomb, *Analyzing Character: The New Science of Judging Men: Misfits in Business, The Home and Social Life,* 1916.

3. Katherine M. H. Blackford and Arthur Newcomb, "Reading Character at Sight", Independent Corporation, 1918.

4. *Physiognomy*, https://en.wikipedia.org/wiki/Physiognomy.

5. Ironically, recent research suggests that *some* personality traits can be correctly judged from physical appearance including self-esteem, degree of extroversion, and religiosity. See Laura P. Naumann, et al., "Personality Judgments Based on Physical Appearance", *Personality and Social Psychology Bulletin* **35** (12) 1661-1671 (2009). Usually it is possible to determine these things simply by chatting briefly with a person. It is not clear, moreover, how much of this is a self-fulfilling prophecy. If, for example, people have a tendency to think an introvert should look a certain way, a given individual may come to be an introvert partially because that is what people expect him to be based on appearance and/or because he himself thinks he looks like an introvert.

6. Roger G. Johnston, Eric C. Michaud, and Jon S. Warner, "The Security of Urine Drug Testing", *Journal of Drug Issues*, **39**(4), (2009), http://jod.sagepub.com/content/39/4/1015.abstract.

7. Roger G. Johnston, "What Alligators and Russian Dopers Can Teach Us About Security", http://tinyurl.com/hxddv72.

8. See, for example, Liz Ryan, "Why Does Everyone Hate HR?", http://www.forbes.com/sites/lizryan/2015/06/05/why-does-everyone-hate-hr/#5b73697d28a1, and Fast Company, "Why We Hate HR", http://www.fastcompany.com/53319/why-we-hate-hr.

Enhancing Safety and Security Interfaces to Improve Radioactive Source Security in Canada

Raphaël Duguay, M.Sc., PSP®

Canadian Nuclear Safety Commission, Nuclear Security Division
raphael.duguay@canada.ca

Abstract

The Canadian Nuclear Safety Commission (CNSC) plays an important role in ensuring that safety and security objectives are harmonized. In doing so, the CNSC's role in securing radioactive sources ensures that safety and security can work together without impeding one another. The Canadian approach emphasizes the importance of safety and security interfaces while also recognizing the societal benefits arising from the safe and secure use of radioactive sources. This paper highlights the actions taken to enhance these interfaces to improve the security of high-risk radioactive sources in Canada. It discuses Canada's implementation of new security requirements under Regulatory Document REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources.* It will also present CNSC's new approach to regulatory activities in this area (which was adopted in 2013) to strengthen safety and security interfaces and oversight by having safety inspectors conduct additional security specific inspections during their regular inspection cycle, supplementing the work performed by security inspectors.

Key words: radioactive source security, safety and security interfaces

Acronyms:

CNSC:	Canadian Nuclear Safety Commission
DSS:	Directorate of Security and Safeguards
IAEA:	International Atomic Energy Agency
IPPAS:	International Physical Protection Advisory Service
NSSR:	National Sealed Source Registry
REGDOC:	Regulatory Document
RSS:	Radioactive Source Security

1. CNSC regulatory approach on security of radioactive sources

Context

In 2013, the CNSC adopted its Regulatory Document 2.12.3, *Security of Nuclear Substances: Sealed Sources* (REGDOC-2.12.3)[1] to implement security requirements for high risk radioactive sources in use, storage, and transport. The purpose was to align domestic practices with international recommendations set out in the International Atomic Energy Agency (IAEA) Code of conduct on the Safety and Security of Radioactive

Sources [5] and the IAEA Nuclear Security Series [6] [7] and to protect these materials from unauthorized removal, sabotage, and malicious use. In order to implement these new requirements, licensees with category 1 and/or 2 high risk radioactive sources were given two years to conduct their gap analysis and implement new security measures to meet these new requirements. For licensees with category 3, 4, and 5 radioactive sources, a five-year implementation phase was given to provide sufficient time for the operators to adopt a risk-based approach.

During the implementation of these new security requirements, CNSC staff identified areas to improve safety and security interfaces. In addition, the CNSC recognized the need to implement more robust processes, procedures, and tools to facilitate internal exchange of information. As a result, specific and targeted training on radioactive source security was developed for safety inspectors from different divisions within the CNSC to provide them with the knowledge and skills required to conduct limited scope security inspections and enforce these new requirements.

The training course development identified 18 learning objectives and followed a systematic approach to training. Overall, the objective of this basic security training course on radioactive sources was to:

- increase participants' understanding of the need to protect high risk radioactive materials based on the consequences of their possible malicious use
- inform participants about the key CNSC requirements from REGDOC-2.12.3 and guidance on the security of radioactive sources
- inform participants about the fundamental security principles of physical protection and their application to radioactive sources
- train participants on key CNSC procedures and processes to:
    - prepare and conduct security inspections
    - protect confidential/sensitive information
    - interface and communicate with security experts when needed.

Finally, it was identified that more transparent and enhanced communication strategies were needed within the organization to enforce these requirements and to provide more awareness for licensee stakeholders. As a result, the need to build more robust partnerships between safety inspectors, licensing staff, transport experts, and security inspectors was identified. These relationships were paramount to ensure adequate financial and human resources were available in the long term for their sustainability, and to ensure that adequate verification activities were conducted during field inspections and during their licensing process.

A Strategy Focused on a Performance-Based Approach

During the implementation phase, the CNSC focused on a performance-based strategy by working with industry to assist in identifying potential solutions that could be integrated into licensee operations without negatively impacting safety. Security experts from the CNSC conducted a series of consultations, site visits, and outreach activities to discuss operational experience, share good security practices and assist in guiding licensees in meeting compliance criteria. In addition, CNSC staff published

information in industry newsletters and continued its effort to disseminate tips and guidance on radioactive source security (see figure 1 and 2 for examples).

FIG. 1. Posting frequently Asked Question on security requirements on CNSC website.

FIG. 2. Published articles on security of radioactive sources in 2016 special industry newsletters[2]

2. Enhancing safety and security interfaces to protect high risk radioactive sources

After the requirements for security of radioactive sources were approved in May 2013, CNSC staff from the Nuclear Security Division (NSD) established a partnership with other divisions responsible for safety inspections, licensing, and transport. To enhance interfaces, the following initiatives were implemented:

CNSC Safety and Security Interfaces for Radioactive Source Security (RSS)	
Management Level (Director General)	High-level management support through a signed **communication protocol** between the Directors General of the Directorate of Security and Safeguards and the Directorate of Nuclear Substances Regulations that defines security criteria to exchange sensitive information and other requirements for clear lines of communication.
Management Level (Directors)	Middle Management –Director level support of implementation by defining clear **roles and responsibilities** for inspectors and security specialists from different divisions; divisional **inspection procedures** revised to include security.
Staff Level	**Working Group** (WG) on Radioactive Source Security with

(Subject Matter Experts)	representatives from all relevant safety, licensing, transport and security divisions with a clear objective to handle operational issues and challenges, exchange information and coordinate compliance activities. The WG meets quarterly, has terms of reference, rotating chair and disseminates minutes to all stakeholders.
Staff Level (Inspectors)	**In addition, several joint programs were developed, including:** • **A joint safety/security inspection** program • A **basic security awareness training** as a requirement for all inspectors as part of their inspector qualifications • **Specific inspection procedures, guidance and checklists** • **Shared communication tools on security plans and security inspections.**

FIG. 3. Multiple levels of safety and security interfaces

Figure 3 shows that safety and security interfaces have been enhanced at various management and staff levels. The development of a joint safety/security inspection program helped to create more robust relationship between safety and security divisions, and to increase communication and sharing of information internally and create a synergy. This process also facilitated security staff to contribute to safety programs and vice-versa. An output of these interfaces allowed inspectors to share inspections techniques and tools and to align internal inspection procedures and inspection templates to have a more harmonized and consistent approach.

Basic new security awareness training course for safety inspectors

To facilitate the joint safety/security inspection program, a new security training course was developed by a training specialist and a security expert for safety inspectors following a systematic approach to training. This course was designed to address the specific needs of each division involved in security inspections and included a review of key shared communication mechanisms and tools between safety and security. The classroom training was bolstered by the safety inspector's shadowing security experts during field inspections whenever possible—helping to enhance open communication channels between safety and security staff. This was integrated into the Inspector Training and qualification program.

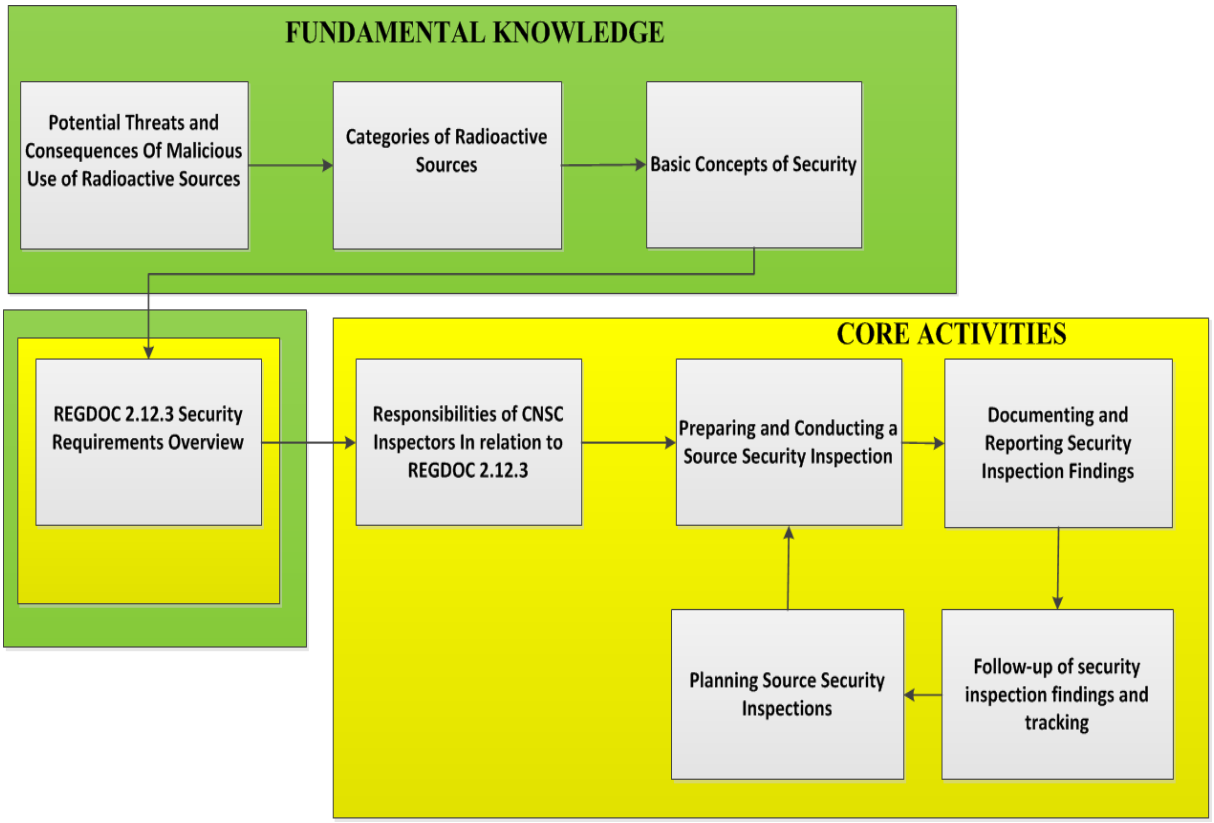

FIG. 4. Basic Security Awareness Training Modules

Security inspection procedures, checklist and shared communication tools

At the operational level, the revision of procedures, guidance, and security inspection worksheets were updated for each division responsible for conducting basic compliance inspections under this safety/security partnership. Inspection tools and procedures were restructured to perform combined safety/security inspections. It was therefore necessary to develop clear expectations for new requirements to assist safety inspectors and provide guidance on how to assess compliance and how to handle confidential information in the field. These tools were integrated into the training developed. such as the shared database for tracking the status of facility security plans and security inspection findings. During this process, protecting sensitive and classified information was an important consideration that could not be compromised. For example, specific procedures were developed and training delivered to appropriate staff.

Implementing a risk-based inspection program for radioactive source security

The implementation of this enhanced safety and security partnership allowed the CNSC to increase the number of combined safety/security inspections at facilities with high-risk radioactive sources conducted by safety inspectors. As a result, more security inspection findings and data were collected with the intent that it could be analyzed to determine trends in deficiencies and gaps in understanding regulatory requirements. This data is used to inform and plan future compliance and outreach activities. For example, in 2013 there were approximately 50 security inspections. In 2015, there were 217 security inspections conducted by safety inspectors in addition to 35 joint inspections with security inspectors. This approach allowed CNSC staff to adopt a risk informed decision process and to focus their efforts where they were needed the most. The data collected during security inspections also assisted in identifying areas where more communication and awareness is needed.

This approach also enabled NSD experts to have more "eyes and ears" in the field and adapt their compliance strategy and efforts toward focusing on new licensees, new locations, or licensees with poor security compliance history or identified vulnerabilities as noted by inspectors. As a result, this approach allowed NSD to focus its resources on higher-risk areas and establish an inspection program based on specific risk factors (e.g., large inventory and activity of radioactive sources held by the licensee, poor compliance history for security inspections, an inadequate facility security plan, or relevant threat information). Overall, having safety inspectors trained to conduct security compliance inspections allows a more sustainable program to enforce requirements and verify compliance in the field. As a result, this synergy allowed the CNSC to enhance their radioactive source security inspection program. However, because the safety inspectors are not security experts or physical protection specialists it was important to emphasize during training and implementation that they can, and should, request expert technical support whenever needed.

In October 2015, CNSC hosted an International Physical Protection Advisory Service (IPPAS) mission as the federal nuclear regulator responsible of safety, security and safeguards. The IPPAS team, composed of 10 experts from nine nations and from the IAEA, reviewed Canada's nuclear security-related legislative and regulatory regime for nuclear material and nuclear facilities, as well as the security arrangements applied to the transport of nuclear material, the security of radioactive material, and associated facilities and activities, and the information and computer security systems in place. The report with only minor redactions to protect sensitive information was posted on the CNSC website as part of its commitment for transparency a. In the report [8], the IPPAS team highlighted the importance of the CNSC implementation of REGDOC-2.12.3, *Security of Nuclear Substances: Sealed Sources*. The team also emphasized the significant safety and security interfaces between different directorates and divisions as well as the effort of the CNSC to increase cooperation and interfaces between the two disciplines to enhance radioactive source security domestically.

3. Current challenges and path forward

National threat assessment on radioactive sources and challenges

In order to meet the recommendations of the IAEA Code of Conduct [5] and the IAEA Nuclear Security Series [7], the CNSC conducted an updated national threat assessment for radioactive sources in 2015. This threat assessment was performed in collaboration with the national police service and focused mostly on external threats (e.g., terrorism). During this project, multiple challenges were faced such as issues with:

- including all relevant threat scenarios related to the malicious use of radioactive material (e.g., international transport, use of insider threat)
- acquiring adequate resources to collect and analyze data on past events domestically and worldwide
- verifying accuracy and adequacy of threat information on past incidents
- consulting relevant stakeholders including industry representatives

- sharing classified information with industry stakeholders due to lack of stakeholder security clearance, staff rotation and inadequate communication platforms (i.e., encrypted networks)

In this latter area, the CNSC continues its efforts to determine solutions to share relevant threat information with relevant stakeholders.

The following are a few examples of initiatives to share information that have proven to be effective to date:

- participating in annual industrial radiography meetings to provide unclassified updates on nuclear security
- sponsoring the security clearance of individuals responsible for managing large radioactive source inventories at their facility
- developing scenario based threats and conduct of table-top exercises and testing with relevant stakeholders to test for timely and effective communication and coordination.

The need for additional security awareness and guidance to facilitate implementation

During the implementation phase, there were many requests from operators to get additional guidance on trustworthiness and reliability verification for individuals with unescorted access to high-risk radioactive sources. Some licensees needed more time to consult unions, legal advisors and human resources. Also, there were issues and limitations identified in conducting criminal record checks for international students and foreign workers.

Moreover, often operators are radiation safety experts, physicians, or end-users and lack the knowledge and expertise on security matters. They struggle with limited resources in their operating environment where people and financial resources are often strained and are competing with other priorities. Many operators requested additional guidance on security practices to help them improve their security program and find the best cost-effective solution. As a result, NSD staff identified that more security awareness and guidance was, and continues to be needed for all relevant stakeholders including operator staff, security personnel and off-site police forces.

Focusing on Category 3, 4 and 5 Sources

Following the initial campaign on licensees with categories 1 and 2 sources from 2013 to 2015, CNSC staff continue their efforts to reach out to facilities with aggregate quantities (categories 3 and 4). In 2018, REGDOC-2.12.3 will become a license condition for licensees with category 3, 4, and 5 sources, and therefore communication and outreach activities are planned to inform the industry on security requirements and expectations.

4. Conclusions

Establishing a partnership between safety and security provided many benefits for the CNSC. The analysis on security inspection findings before and after the implementation of new security requirements [1] shows a positive trend for security in different sectors

[3][4]. To increase awareness and compliance, CNSC staff also developed strategies to ensure clarity of expectations, including focused outreach and a newsletter on security of sealed sources.

As a result of these interfaces, more security inspections are conducted in the field and security is now part of safety inspections for high-risk radioactive sources. The training provided to safety inspectors and the increased visibility of security during inspections, outreach, and communication activities helps to promote stronger security and safety interfaces and to improve security culture. To continue to improve, better sharing of threat information with industry, and future implementation of exercises, drills, and testing of security practices at facilities and during transport are needed.

Acknowledgements

I wish to acknowledge the valued contributions and support over the last six years of the staff from the Directorate of Nuclear Substances Regulations in particular S.Faille, K. Murhty, H.Rabski, P.Fundarek, F.Dagenais, M.Thériault, R.Obuchi, T.Gulinski, N.Babcock, P.Matthews, M.Broeders, and R.Kosierb and the NSD team in achieving successful delivery and outcomes of these programs. Thank you also to Mr. R.Awad who proposed the idea for this paper and supported our initiatives since the beginning.

References

[1] CANADIAN NUCLEAR SAFETY COMMISSION *Regulatory Document 2.12.3. Security of Nuclear Substances: Sealed Sources*

[2] CANADIAN NUCLEAR SAFETY COMMISSION Directorate of Nuclear Substances Regulations Newsletter Special Edition 2016 on security of radioactive sources.

[3] CANADIAN NUCLEAR SAFETY COMMISSION Regulatory oversight reports on the use of nuclear substances 2014

[4] CANADIAN NUCLEAR SAFETY COMMISSION Regulatory oversight reports on the use of nuclear substances 2015

[5] INTERNATIONAL ATOMIC ENERGY AGENCY (2003). Code of Conduct on the Safety and Security of Radioactive Sources. Vienna, 2003. Available online at: www-pub.iaea.org/books/IAEABooks/8616

[6] INTERNATIONAL ATOMIC ENERGY AGENCY (2009). Nuclear Security Series No. 11, *Security of Radioactive Sources*.

[7] INTERNATIONAL ATOMIC ENERGY AGENCY (2011). Nuclear Security Series No. 14, *Nuclear Security Recommendations on Radioactive Source and Associated Facilities*.

[8] INTERNATIONAL ATOMIC ENERGY AGENCY (2015) International Physical Protection Advisory Service Mission to Canada Unclassified Report

Principals' Perceptions of Physical Security and Armed Personnel: An Exploration of New Jersey School Administrators' Views on Active Shooter Countermeasures

Brian P. Kelly
Farmingdale State College, State University of New York
2350 Broadhollow Road, Farmingdale, NY, 11735, kellyb@farmingdale.edu

Abstract

Violence in K-12 schools is a phenomenon which contains challenges and controversy, particularly when determining a proper response. School principals in New Jersey face a predicament when formulating the best methodology to provide a safe environment for their students and faculty, while simultaneously creating an atmosphere that is conducive to education. In this multiple case-study, New Jersey suburban public school principals' perceptions of physical security and armed personnel are presented, and discussed. To achieve this task, I interviewed 21 school principals to collect pertinent evidence about their discernment of utilizing physical security and armed personnel in their schools, as well as explore which areas of implementation are best as it pertains to school safety in these specific New Jersey school districts. Qualitative data were derived from the respondents, and coded from extensive narratives accordingly. The results of this study provided valuable information, including (1) the various security applications that were most desirable to the principals relative to deterring school violence, and (2) the overarching concept of current mandates and protocols which the New Jersey school administrators must adhere to in the area of school security.

Key Words: active shooter, physical security, principals, schools, policy, technology

1. Introduction

History has shown that schools can be portrayed as emotionally charged environments where frustrated students, as well as staff, commit acts of violence. School leadership has emphasized safety with regard to dealing with school violence. Developing procedures that make schools safer places to learn seems an obvious need, yet such measures can lead to a false sense of security. Focusing only on physical security measures sets the precedent for evasion of these measures rather than prevention of the underlying reasons for violence in schools in the first place (Blanchfield, 2013).

In an era considered to be and often referred to as "Post 9/11", an alteration in thought processes within school districts across the nation, and perhaps even the world, calls for security-minded decision making within many educational infrastructures, regardless of the jurisdiction examined. A negative school climate can become a breeding ground for violence and polarization in schools, while a positive climate can engender nonviolence and cooperation (Blanchfield, 2013). Thus, leaders of the educational institutions, i.e., the school principals must be effective in their decision making for school safety measures. Last year (2015) brought 332 mass shootings in the United States, and 13,476 gun-related deaths, many of which occurred in K-12 schools.

Since January of 2014, New Jersey has had 23 mass shootings, 776 gun-related deaths, and 12 police officers killed or wounded by gunfire (Gun Violence Archive, 2016). K-12 educational environments are repeatedly included in these statistics. New Jersey school principals possess the authority in public school districts to dictate the level of security measures which can be utilized, barring financial constraints only. In this paper, many aspects encompassing combatting, controlling, and preventing gun violence in New Jersey suburban public school districts are examined, as well as their direct correlation with security operational procedures, the use of armed personnel in schools, and physical security.

2. Conceptual Framework

Abraham H. Maslow's hierarchy of needs sheds light on these critical issues. Maslow believed in order for an individual to reach self-actualization, he/she had to first meet

other needs (Mittelman, 1991). Physiological needs are the physical requirements for human survival; safety needs are the state in which their physical needs are relatively satisfied. The individual's safety needs take precedence and dominate behavior. Principals must assess the needs of their specific educational environments. Furthermore, New Jersey suburban public school principals must determine if the basic needs, as prescribed by Maslow, have been achieved in order to progress to more advanced needs, especially for students and faculty.

3. New Jersey Model School Security Policies

In 2007, Ann Milgram, the Attorney General of the State of New Jersey, issued a directive to all county prosecutors pertaining to the Model School Security Policies, in conjunction with the organization Securing Our Schools for a Better Tomorrow (SSBT). The directive instructs all law enforcement agencies in the state of New Jersey to have and maintain policies enhancing school security and safety (Attorney General Law Enforcement Directive 2007-1). Through these policies, all New Jersey K-12 schools were then authorized to carry out protocols set forth by the state, often in conjunction with law enforcement, or under the supervision of the lead administrator of the institution, typically the principal. New Jersey public school principals received training in various areas relative to security, and are responsible for bringing the mandated training back to their faculty and staff, institute the necessary protocol, and ensure that the criteria are followed. For example, two drills per month, including one fire drill, and one drill of an additional category in the area of security counter measures, must be carried out, and documented with the school district, the local police department in that district, as well as the New Jersey Department of Education, who then reports all results and outcomes to the Office of the Attorney General in the state of New Jersey (Attorney General Law Enforcement Directive 2007-1).

3A. Active shooter

The United States Department of Homeland Security (n.d.) defines an active shooter as “an individual actively engaged in killing or attempting to kill people in a confined and populated area, typically through the use of firearms. Klein (2005) asserted that popular

discourse addressed school shootings obsessively but continued to omit the role gender plays in these crimes.

3B. Lockdown

New Jersey school officials must immediately notify law enforcement and report the reason for the lockdown, if and when this type of scenario takes place. Law enforcement has a responsibility to take the necessary actions to address and remove the threat, investigate the situation, and inform the school officials of their findings (Attorney General, 2007). After the Columbine tragedy, many schools introduced policies or increased existing security measures with the intention of reducing the occurrence of overall violence (Jackson, 2002). For the last decade, New Jersey public schools have been one of many state departments overseeing educational institutions that have led by example in the area of school safety practice and policy effectiveness.

3C. Bomb threats

According to the Attorney General's Directive 2007-1, all New Jersey school principals must be prepared to encounter security incidents, including but not limited to bomb threats. This type of protocol is common, as many states are in alignment with directives such as 2007-1. On September 16, 2015, Ahmed Mohamed, 14, who was arrested after his teachers in Irving, Texas, mistook his digital invention for a bomb (Golgowski, 2015). Mohamed stated, "I built a clock to impress my teacher; but when I showed it to her, she thought it was a threat to her so it was really sad that she took the wrong impression of it" (Golgowski, 2015). The teacher confiscated the clock before Ahmed was called into a meeting with the principal and five police officers. All charges in the "naive accident" were dropped and the case has been closed, Irving Police Chief Larry Boyd said at a press conference, noting "the reaction would have been the same regardless" of Ahmed's race or religion. Earlier, police said it could have been mistaken as an explosive device, prompting them to weigh charges of making a hoax bomb (Golgowski, 2015).

4. Constitutional Applications

The New Jersey School Search Policy Manual (1998, p. 13) defines a search as "conduct by a government official that involves an intrusion into a student's protected privacy interest." In New Jersey v. T.L.O. (1985), the landmark decision on school searches, the Supreme Court ruled that school officials act in *loco parentis* and, as such, are only required to have reasonable suspicion, a standard that is less than probable cause but higher than arbitrarily, to conduct a search and to seize any contraband recovered (Holtz, 2014).

Staunch supporters of gun rights point to the various societal causes of school shootings, rather than the tens of millions of firearms in the hands of the citizenry. Those who blame this unprecedented violence on the prevalence of guns have attempted litigation to hold gun manufacturers liable, and they claim that there is no absolute right to own a gun.

5. Participants

The New Jersey suburban public school district factor group that was sampled, District Factor Group 'GH' (New Jersey Department of Education, 2004), was comprised of 76 total school districts. From this population, 8 school district superintendents responded. These 8 districts contained 46 principals within the various K-12 public schools.

From the possible 46 school principals solicited, 21 (n=21) principals voluntarily responded. Figures 1-3 depict the following demographic data on the subjects who responded and were interviewed: (1) Participant's Age, (2) Gender of School Principal, and (3) Years as a School Principal.

I believe that these demographic data played a part in the content of the responses to the interview questions, as well as the overall nature in which security is emphasized and implemented in each of the suburban public school principals' districts. A further examination of these data will be presented later in this paper.

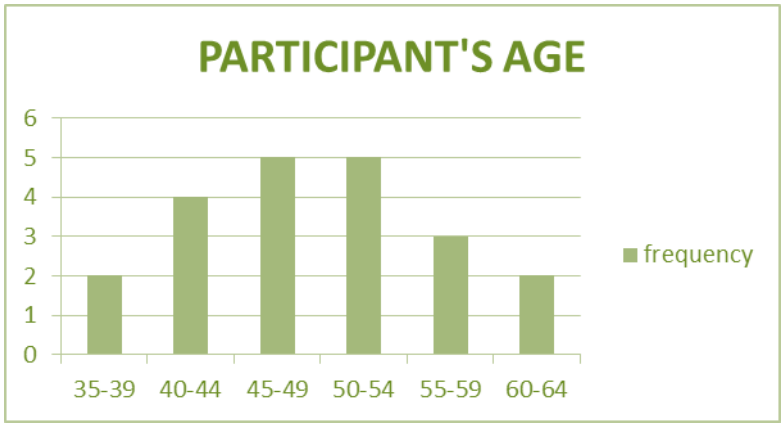

Figure 1 - Ages of Participants

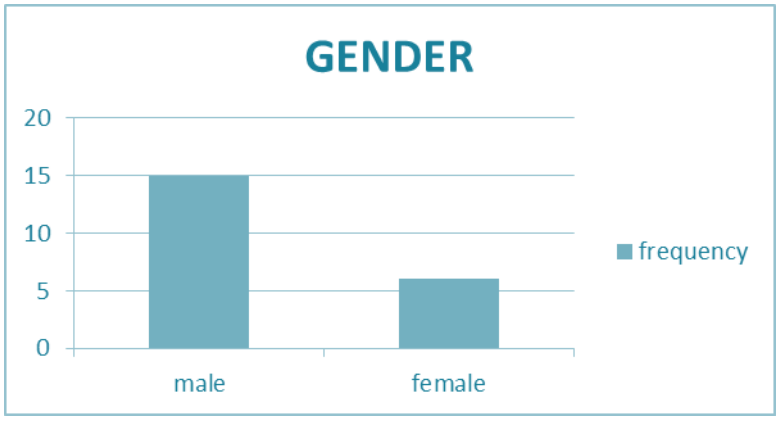

Figure 2 - Gender of participants

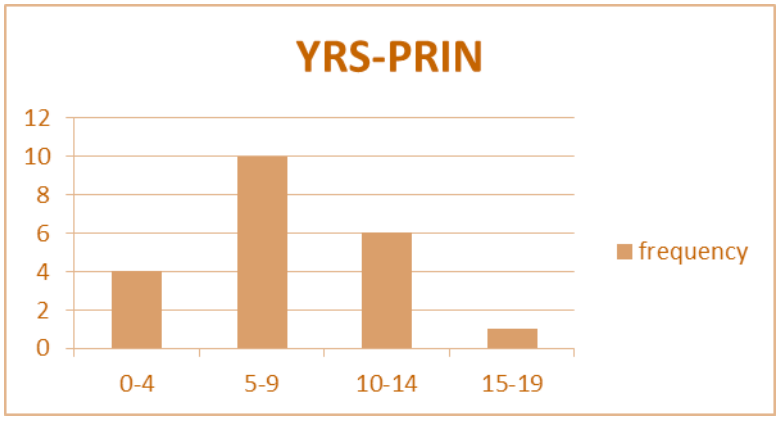

Figure 3 - Years as a School Principal

6. Settings

The public school districts that granted me permission to conduct this study were West Orange, Fairfield, Edgewater, Frelinghuysen, Springfield, Paramus, Fair Lawn, and Roxbury. According to the Uniform Crime Report for New Jersey, each public school district that participated in this research study possessed a particularly low rate of violent crime.

The schools within these districts consisted of 12 elementary schools, 5 middle schools, and 4 high schools, for a total of 21 public schools. This particular district factor group (GH) was selected for its socioeconomic status, and the size of school districts themselves, coupled with other variables in contrast to an earlier study (Reyes, 2014), including but not limited to median household income and an urban versus suburban genre. This previous study (Reyes, 2014), in an all urban public school district, utilized only elementary public school principals, where there were 12 in total, and located in district factor group (A), as delineated by the New Jersey Department of Education.

In this current 2016 study, no township where a suburban public school district participated had a shooting in any of their schools (New Jersey State Police, 2014), and only 2 of these districts that participated were located in townships in New Jersey where a murder had occurred (New Jersey State Police, 2014). Specifically, the towns of West Orange and Roxbury were the locations where murders had occurred.

As part of this research, I chose to conduct the face-to-face interviews for all New Jersey Suburban Public School Principals who responded to my Letter of Solicitation for my research study. I n chronologically documented sections written below, specifically 7 through 9, narratives are cited to exhibit the suburban public school principals' ideologies, opinions, and actions each takes pertaining to security, and areas of emphasis the school principals noted when communicating to me their priority in their overall vision of school safety in the suburban public schools they operate.

7. Security Policy and Procedures- Participant Narratives

Every New Jersey suburban public school principal was vehement about their staff and students being prepared though conducting active shooter drills, lockdown drills, shelter in place drills, bomb drills, and fire drills, as mandated by policy, and additional

procedures written by various administrators. Commenting on the security procedures and the actual drills the principals carry out, principal **D1-P2** echoed the sentiment that all the principals offered: "We do that, you know, once a month we have to by law, it's a statute that we conduct lockdown drills. So there's a variety of situations. They're defined for lockdowns; but here, and I figure I can speak for the rest; we take every lockdown as a lockdown in which it's extremely serious. The kids are well-practiced at what they're doing. The teachers know exactly what they're doing; and, you know, no room is cleared until I, the principal, walk in and clear that room." (February 23, 2016). **D1-P8** also echoed the sentiment: "And where we're located, we tend to have a lot of foot traffic. We have safety drills in place. We have tabletop procedures where the police are involved. And recently, we had NBC News come to our school—I think it was maybe two years ago, doing safety checks on different schools. And we passed with flying colors." (March 15, 2016). **D2-P2** said, "I'm pretty confident with our procedures in place because our school resource officer also works for the Department of Homeland Security under the Department of Education. Actually, he worked for the Department of Education under the Department of Homeland Security. He is the one that actually was part of the team that would go out into the state and monitor the drills. So, he would walk in with the state police. They would call lockdown. You know, he worked on writing those plans for the state and then observing them in practice, so I'm pretty confident that we're in good shape." (March 11, 2016).

D7-P1, similar to other principals interviewed, identified the importance of having all exterior doors monitored and the challenges that accompany that. "We also have greeters who are at the desk. They sign everybody in and out. We have only two entrances open. We have 36 exterior entrances and exits in this place so we only have two of them that are open. The rest are locked. If we need to bring somebody out of class, we'll call them with their radios and we have full, you know, our radios are fully—everybody in the building that has got any kind of administration or [is] responsible for safety has got a radio. Custodians, we make sure everybody communicates when they need to communicate; and if something happens, you know, you've got five people there in an instant." (March 14, 2016). **D1-P3** stated, "We have a lot of workers that come in and out of the building, vendors and custodians. We go out there and meet them or whatever the case may be. We actually did take some additional measures with our current superintendent.

He made sure we all had passkeys. All staff members were to have passkeys to enter the buildings. So we no longer have to necessarily buzz in staff throughout the course of the day, and what was happening is you would leave a door unlocked in the mornings so the staff can constantly come in, or whatever, or staff would keep a door ajar or jimmy a door to some degree to make sure that it stayed open. Now, the need for that is no longer. We have three doors, four doors actually that can be accessed through the staff's passkeys." (March 2, 2016). **D5-P2** explained, "We have the bell system and we have the intercom in the office for when a visitor comes to the door. They ring the bell. There's a camera and whoever answers the phone asks who it is and asks them if they're not already in front of the camera to step in front of the camera so that we know who—we can identify the person before letting them in." (March 9, 2016). The principals interviewed experienced satisfaction in the vigilance through their policy and procedures. Most principals acknowledged all, and implemented within the scope of their authority, additional policies that allowed each of them to advance the security of their school, specifically regarding identification upon admittance into the school.

8. Armed Personnel- Participant Narratives

Despite the use, and constant evolution of security policy, most of the 21 principals paused temporarily when asked, "What personnel should be armed, if any?" **D5-P3** paused, thought about the question and stated, "No portion of the personnel should be armed. We don't want to live in fear. Our children will feel they need to rely on gun safety; it's about education. And I believe it would have a more negative effect overall and would send a different kind of message." (March 17, 2016). **D2-P2**, when asked who should be armed, answered, "I believe there should be someone armed. It does make a statement when I walk into my daughter's school. She's in middle school." (March 11, 2016).

One principal, **D6-P1**, was adamant that at this time, having any person in a school carrying a weapon is vital. **D6-P1** said, "I'm all for armed personnel, including a principal, if need be. Obviously a full-time cop would be a perfect scenario, and I definitely think it would have a positive effect. I believe security without a weapon is a waste." (March 3, 2016). Another Principal, **D2-P2**, said he felt comfortable with an administrator being armed with a firearm for security reasons. "I'd really like to talk about my view of a

principal being able to carry. I've had many discussions with the police department on this because as a principal, you know, you really feel responsible. I have 400 kids and 100 staff members because, you know, with the little ones we have a lot of aides. I feel very responsible." (March 11, 2016).

9. Physical Security- Participant Narratives

When the principals were interviewed for this study, each was asked about the safety of their school, students, and faculty, as well as in what areas they needed to ensure school safety. One frequent topic was physical security, which included security guards, surveillance cameras, doors and their locks, and a buzzer or bell for the front entrance**.**

The research interview question asked, "What options are available for a safe and secure school other than armed personnel?" **D2-P2,** in answering this question said, "We're fortunate to have metal doors, metal doorframes. Steel doorframes and we have the magnets so every door is locked at all times. All the teacher has to do—you don't have to fumble for a key. Just slide the magnet. My door is a little different; every classroom door they will frost from here down so you will not be able to see in at all. We have one I can show you before you leave. Then from here up it's just a piece of heavy duty black canvas or felt that has a snap so it snaps up so you just snap and let it go. So, no more rolling the shades because they're all breaking." (March 11, 2016).

All the principals interviewed in this study were very serious and concerned with the physical security of their schools. **D5-P3** said, "We have a card system to access the building. If someone got access to the key card I could deactivate the whole building with my master key card. We have surveillance; we were given a grant to update all cameras we try to educate the parents." (March 17, 2016).

Another area where principals expressed concern was the ability to have a surveillance system in their school. **D4-P1** said, "Well, what we're looking towards right now—we only have one camera and it doesn't even archive. This is my first year here so that's something we're addressing over the summer in our budget—to make sure there's cameras throughout the building and even internally. The problem with cameras, too, is it's more just, like I said; it's almost like a false sense of security for families because I mean the police can tap into it. So, if there were a hostage situation or something of that nature,

they could use it to identify; but the problem is with these shootings, they're so quick. They're not sitting there for hours holding anybody hostage or sitting there blowing people away. So, I mean, the community wants the cameras and I understand why but it's, again, it's kind of like a false sense of security. It helps us immediately identify people who want to come in but I think if someone wants to come in with bad intentions, they're going to come in regardless. We're also addressing some of the PA systems to make sure that if we call—we have pretty big grounds here. You know, we're rural. So, we make sure our PA systems can reach everybody, especially when the kids are outside for recess. We do have to do a reverse evacuation and bring the kids in or lockdown to make sure the kids come in so they can hear it. We're exploring those lights that show up too, like some of those blue lights that kind of if they went off, the police would know that there's something going on. Even a panic button has been brought up. Then, the capability for our teachers to be able to call a lockdown because right now they're not able to. Only I could. So, if something were to happen to me, nobody else could call lockdown." (March 8, 2016).

Regarding additional security options, as well as the recognition of an imperfect situation, **D6-P2** mentioned, "They've added some kind of a shield, like a bullet proof —you know what I mean? They've reinforced the glass in the front. After that terrible shooting in Connecticut, they reinforced the glass in the front vestibule there. The camera systems are all new. All of the schools have like—we have like a monitor now where—like this incident that I told you about with this lady, that whole thing we can see it on film. You can see it on film, but what else? The doors are locked. The doors are manned. As best as we can, people are not allowed in the school; but the problem is sometimes at dismissal and at arrival." (March 3, 2016).

Another issue that brought concern to the school principals was money allotted for security in their school. **D7-P2** noted, "It would be nice to be able to have a double entry system with somebody who is set at the second door checking IDs. I know a couple of years ago, I read about a school in Chicago. They actually have a police scanner system so that they take the ID through like a bank teller window. They run it through the scanner. It runs through the police records and it identifies whether or not they have a criminal record or anything. I think it was something like $700,000 a year to operate. That's a pipe dream; but if there were some type of capability where we could have that double-entry system

with bulletproof glass, where we could be able to identify through their identification whether or not there's a record on them or at least keep a record of them in the building so that should anything happen, we know who that perpetrator or the aggressor is. I would also love to be able to alarm every set of doors that we have in the building. Again . . . it would be multiple purposes. So if we do have somebody who flees and gets out a door, we now know where they left from. So I think that for something like alarming all of the doors, that would be a multiple benefit" (March 15, 2016).

All of the principals interviewed placed great importance on having the proper physical security in the schools, and that it should be modernized. Throughout the interviews, the principals spoke of physical security as a top priority for the security and safety of the students and faculty. All principals interviewed also emphasized access control procedures for outside personnel wishing to gain access into the schools. This access control was intended to prevent, combat, and control school violence, specifically a shooting on school grounds.

The principals identified physical security of the school as a major component in keeping the students and faculty safe and secure. Physical security of the building, specifically door locks and buzzers/bells for better safety/security, was a recurring theme raised by the interviewees. Gunshot detection systems, high-definition motion-detecting cameras that analyze behavior and identify threats, security film for windows, automatic gates that secure the shooter in a mantrap, and mass notification systems were all touted as some of the best potential solutions for active shooter prevention and response.

Of course, these solutions do not come cheap, and many principals would agree that school budgets should be dedicated primarily to academic technology, books, sports equipment and learning facilities, rather than security systems. The entire total sample population (21) endorsed the current physical security they possess and would welcome even more, if budgetary constraints permitted.

Table 1: List of Research and Interview Questions for the School Principals

Interview Questions
1. What are your concerns regarding a student being a victim or perpetrator of a violent act in your school? 2. What are your concerns regarding a faculty member being the victim or perpetrator of a violent act in your school? 3. What are your concerns with an outsider coming into the school to commit a violent act against a faculty member or student (e.g. parent, etc.) in your school?
1. What safety measures have been instituted to provide for a safe school? 2. What training has been provided for teachers to protect themselves and their students in the case of a perpetrator committing an act of violence? 3. What education has been provided for students to be part of creating a safe environment in school?
1. What personnel should be armed, if any? 2. Does the presence of armed personnel have a positive effect or would it escalate the issues of school violence? 3. What options are available for a safe school, other than armed personnel? 4. What are your capabilities and resources as it relates to physical security?

Table 2 - Identity Codes, Race, and Gender For Study Participants

Participants	Race/Gender
• D1-P1	Caucasian/F
• D1-P2	Caucasian/M
• D1-P3	AfricanAmerican/M
• D1-P4	AfricanAmerican/M
• D1-P5	AfricanAmerican/M
• D1-P6	Caucasian/F
• D1-P7	Caucasian/M
• D1-P8	Hispanic/M
• D2-P1	Caucasian/M
• D2-P2	Caucasian/M
• D4-P1	Hispanic/M
• D5-P1	AfricanAmerican/M
• D5-P2	Caucasian/M
• D5-P3	Asian/F
• D6-P1	Caucasian/F
• D6-P2	Caucasian/F
• D6-P3	Caucasian/M
• D6-P4	Caucasian/F
• D7-P1	Caucasian/M
• D7-P2	Caucasian/M
• D8-P1	Caucasian/M

This six-question instrument, not used in the original study, was implemented as a precursor to the actual field interviews with the principals. Its results allowed me to formulate additional data regarding principals' perceptions of physical security and armed personnel.

Table 3 - School Principal's Demographic Data Sheet

1. Your title is school principal:	Yes ___ No ____
2. Your age is:	Response:
3. Your gender is:	Response:
4. How many years do you possess in the area of education?	Response:
5. How many years do you possess as a school principal?	Response:

The following data were extracted from the responses provided by the principals, based on the demographic data sheet in table 3.

Table 4 - Data derived from the School Principals' Demographic Sheets

Principal Demographics	Total Number per Category
• Principals	21
• Males	15
• Females	6
• Over 30 Years Old	21
• Over 40 Years Old	19
• Over 50 Years Old	17
• Over 60 Years Old	2
• Years as Principal (≥ 5)	17

10. Results

After a thorough analysis of the narrative data, I was able to observe, formulate, and document various themes that were relevant to this study.

The previous study included 12 participants, who were principals of only elementary schools, in all urban districts (Reyes, 2014). The 21 principals from the suburban districts who participated in this current research study were divided amongst the following grades levels: elementary, middle, and high schools.

One of three uniting themes of all the responding school principals in this current research study were the security-oriented Policy and Procedures of their suburban public school districts and the New Jersey Department of Education, coupled with the concept of possessing Physical Security, and choosing to utilize armed personnel, or not.

Table 5 - Codes Established by the Author for the 3 Primary Themes Identified in this Study.

Code	Theme	Sub-	Sub-Theme
AP	Armed Personnel	tea	Teacher
		apo	Active Police
		rpo	RetiredPolice
PS	Physical Security	cam	Cameras
		dls	Door Locks
		buz	Buzzer / Bell
		sec	Security
PP	Security Policy and Procedures	acp	Active Shooter Procedure
		ldp	Lockdown Procedure
		shp	Shelter in Place Procedure
		drl	Drill

Of the 21 interviews conducted, Security Policy and Procedures was identified as the number one issue relevant to school shootings and safety, as well as what may be considered in this multiple-case study the primary component necessary to maintain a safe and secure learning environment. The school principals referenced this crucial theme 212 times. Armed Personnel, was referenced 189 times, following Policy and Procedures as the second most dominant theme emerging from the research study. Physical Security followed with 129 instances.

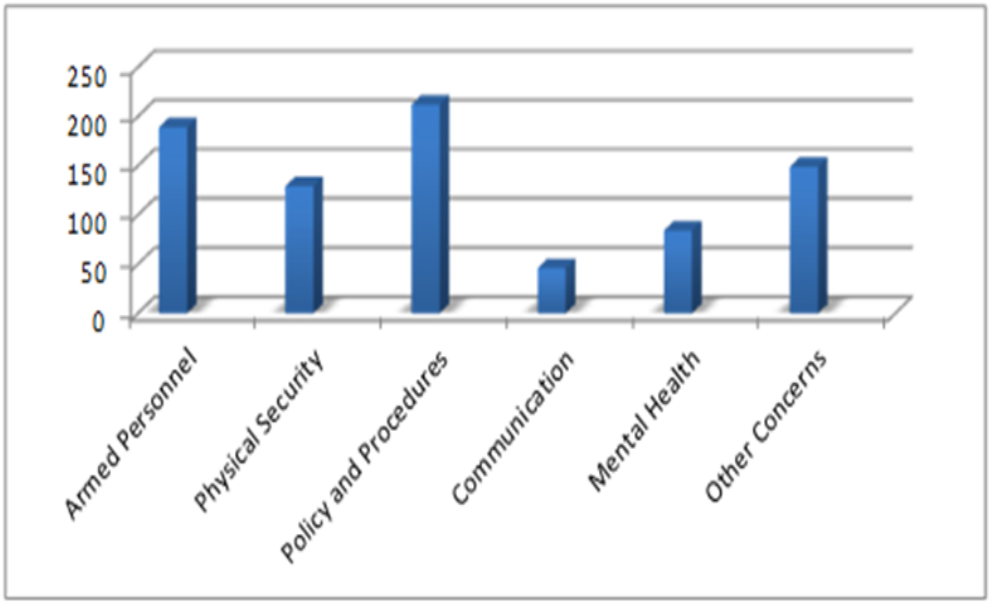

Figure 4 - Prevalence of Security-related Qualitative Data within Suburban Public School Districts: Numeric Responses (2016)

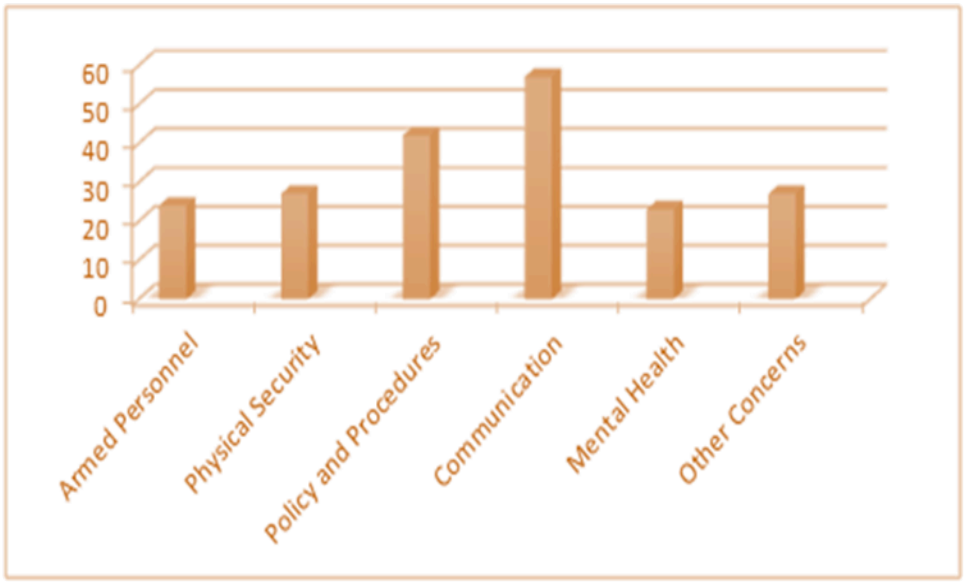

Figure 5 - Prevalence of Security-related Qualitative Data within Urban Public School Districts: Numeric Responses (2014).

These results can be compared to the original 2014 study of one large urban public school district categorized within New Jersey District Factor Group A. For that earlier study, Policy and Procedures was referenced 42 times, Physical Security 27 times, and Armed Personnel 24 times (Reyes, 2014).

Throughout each interview for this multiple-case study, the New Jersey suburban public school principals referred to their policy and procedures to highlight the degree of significance that they place on the safety and security of their students and faculty. Security Policy and Procedures became the primary emergent theme on which they concentrated when answering questions about their faculty and students.

The principals' answers concerning whether armed personnel should be in their schools, were clear and decisive. The twenty-one principals (n=21), who lead the specific New Jersey suburban public school districts within New Jersey District Factor Group 'GH' that participated in this research study, responded frankly based on their schools' needs, as well as how they each felt about guns actually being present in their schools.

All 21 principals, 15 males and 6 females in total, agreed based on the thematic analysis, that Security Policies and Procedures was the primary factor that could contribute towards a safer and more secure school, as well as eventually lead to, if not already exhibited, a better trained faculty and staff and better equipped student population.

The principals identified the knowledge and practicing of policies and procedures on active shooter, lockdown procedures, shelter in place, fire drills, and bomb threats, as valuable tools in providing a safe and secure environment for the students and faculty, on all levels of education pertaining to this study, kindergarten to 12th grade.

Additional results indicate that 4 of the 5 middle school principals endorsed armed personnel (EAP: D1-P3, D1-P7, D7-P2, D8-P1)**,** as well as all 4 high school principals who participated in this study (EAP: D1-P4, D5-P1, D6-P3, D7-P1)**.**

Table 6 - Coded Research Results of Perceptions of Armed Personnel by Gender.

Principal	Theme	Gender	Endorses Armed Personnel in their school
D1-P1	Armed Personnel	F	YES
D1-P2	Armed Personnel	M	NO
D1-P3	Armed Personnel	M	YES
D1-P4	Armed Personnel	M	YES
D1-P5	Armed Personnel	M	NO
D1-P6	Armed Personnel	F	YES
D1-P7	Armed Personnel	M	YES
D1-P8	Armed Personnel	M	NO
D2-P1	Armed Personnel	M	YES
D2-P2	Armed Personnel	M	YES
D4-P1	Armed Personnel	M	NO
D5-P1	Armed Personnel	M	YES
D5-P2	Armed Personnel	M	YES
D5-P3	Armed Personnel	F	NO
D6-P1	Armed Personnel	F	YES
D6-P2	Armed Personnel	F	NO
D6-P3	Armed Personnel	M	YES
D6-P4	Armed Personnel	F	YES
D7-P1	Armed Personnel	M	YES
D7-P2	Armed Personnel	M	YES
D8-P1	Armed Personnel	M	YES

Because the sample sizes are small, it may be impossible to derive a definitive answer as to whether middle school and high school principals endorse armed personnel more than elementary school principals.

Table 7 - Average Age by Gender of Principals Who Did and Did Not Endorse Armed Personnel

Age/Female: EAP		Age/Male: EAP	
yes	no	yes	no
52.5	49.0	47.8	44.5

Table 8 - Average Years as Principal for Study Participants by Gender

Female/YAP	Male/YAP
8.83	6.93

Table 9 - Average Years as Principle for Those Who Endorsed Armed Personnel

Female/YAP-EAP	Male/YAP-EAP
8.25	5.90

The data suggest that the more years of experience a *male* suburban public school principal possesses (whether male or female), the greater the extent of the security integration that will ensue within their school, as well as the greater the perceived need for armed personnel. I am basing this conclusion on the average raw numbers relative to years as a school principal for each male, coupled with the responses I received from the interview questions I asked.

It is also fairly evident that the older a New Jersey Suburban Public School Principal is in this particular district factor group, regardless of gender, the more these particular respondents favor armed personnel within their schools.

11. Discussion

The interviews conducted with the New Jersey suburban public school principals revealed major themes regarding school safety and security. Through the use of case studies, I hope it is possible to develop an understanding of the subtleties and nuances of violence beyond the drama of tragic and dramatic violent events such as school shootings (Blanchfield, 2013). The controversy about countermeasures to school shooters, in and of itself, reveals that the literature characterizes a multitude of attitudes ranging from concepts such as (1) most school faculty and staff should be allowed to be armed in a school, to (2) security-related policies and procedures are essentially a K-12 bible of sorts, and (3) physical security is more pertinent than armed personnel as it pertains to school safety, and what is most conducive to the K-12 learning environment.

This study allowed me to interview 21 Kindergarten to 12th (K-12) grade school principals from New Jersey District Factor Group GH, comprised of suburban public school districts in New Jersey. In comparison to an earlier study conducted in Paterson, New Jersey (Reyes, 2014), that urban public school district contained a much lower socioeconomic status than my research study conducted in 2016, as well as a higher crime rate (Reyes, 2014). As a result of the interviews conducted for this current study, the

critical issues in terms of priority based on the participants' comments are: (1) policy and procedures, (2) armed personnel, and (3) physical security. Significantly, 6 principals vehemently did not want any armed personnel in their public schools. Of these 6, 2 were female, one Caucasian and one Asian. A total of 11 male principals endorsed the concept of armed personnel within their schools. Out of the 4 males who did not support the idea of equipping their schools with armed personnel, 2 were Hispanic, 1 was African-American and 1 was Caucasian.

The New Jersey suburban public school principals in this study have recognized both policy and procedures and the possibility of having armed personnel as their chief concern in providing a nonviolent school for their students and faculty. Many principals also placed significance on ensuring their schools maintained properly operating cameras, door locks, buzzer/bell systems, and a human presence if possible. Most of the principals preferred security personnel to interact spontaneously with people from the outside attempting to enter the building rather than worry about an active shooter. An emphasis was obvious in most interviews that each principal was aware of the vulnerabilities of an active shooter.

The New Jersey suburban public school principals depend on their policies and procedures and drills, mandated and otherwise performed through consistent training: active shooter, lockdown, and shelter in place. The policy that was most important to all principals interviewed was requiring that any person entering their school be escorted to the main office after signing in, as well as being photographed, a procedure that I had to follow every time I entered a school or school facility I visited for this study.

Resulting from the interviews I conducted, all the principals focused on security problems that were of practical concern, where they are the gatekeepers of their professional domain. The principals interviewed were inclined to speak about the physical security of the buildings when discussing the safety of the students and faculty. An additional important factor they identified was human error, such as faculty and staff not securing each and every door throughout the school. Effective Physical Security could potentially eliminate or compensate for some human error.

12. Conclusions

This research study examined the challenges New Jersey Suburban Pubic School Principals face when determining the best methodology for maintaining the safety of their institutions, while simultaneously deciding on what options allow for a more conducive learning environment. Correlating vital concepts such as school security, educational leadership, and security-related technology implementation in suburban K-12 educational environments in New Jersey will allow for a more robust evaluation when making plans to deter violence in schools, and protecting human lives.

The New Jersey suburban public school principals prioritized their school safety strategies through a series of processes based on mandates and their years of experience. They strove to: (1) ensure that the policy and procedures of their school districts and the NJDOE are monitored, especially the conducting of drills; (2) determine whether having armed personnel is conducive to the educational environment; and (3) ensure that physical security, cameras, door locks, buzzers, bells, mobile escorts, and possible security personnel, are present. All buildings in this study had some version of physical security, whereas the 2014 study conducted in the urban public school district located in Paterson, New Jersey did not (Reyes, 2014). The New Jersey suburban public school principals directed their responses to school safety to developing trust with the students and staff, adhering to the safety policies and security-related procedures, performing the appropriate drills, and guaranteeing the building is physically secured to the best of their abilities and the authority which is granted to each principal based on the job specifications in their school districts.

The 6 New Jersey suburban public school principals did not support having any armed personnel in the schools, including law enforcement or retired law enforcement. However, the principals who did endorse the consistent presence of police officers and retired police officers in the schools, were very supportive of them as professionals, and wholeheartedly endorsed arming them.

School security experts caution school officials and law enforcement officers from focusing solely on active shooters, and not having an all-inclusive program that deals with school violence, including active shooters and suicide (Ujifusa, 2012). The principals interviewed in this study specified that the processes used in their schools

remain wide-ranging in their emphasis, being concerned with an active shooter, an irate parent, custody issues, etc.

Nonetheless, every principal expressed that his or her role has transformed a bit since being hired as a principal, where 20 of the 21 administrators held the title of principal prior to the school shooting massacre at Sandy Hook Elementary School, an event that once again altered the way school districts approach security measures. Each principal admitted when discussing those events that they felt anything could occur, specifically referring to something violent in nature. Only one principal, D7-P1, held the title of principal during the school shooting massacre in 1999 at Columbine High School in Littleton, Colorado.

Recommendations for Future Policy and Practice

In my view, New Jersey Suburban Public School Principals should be mandated to conduct bi-annual reviews of physical security statuses in their schools, including examining the need for improvements, as well as future upgrades. At a minimum, resources such as buzzers upon each valid entrance where CCTV camera is present, swipe cards for entrances for all persons, bullet proof glass, classroom air locks, classroom panic buttons and administrative panic buttons via remote controls should be consistently evaluated and experimented with, at the request of the school principals.

School principals should complete a district security budget annually representing the requisition of physical security resources to each superintendent.

School principals should mandate school resource officers from within their jurisdiction's police department; conversely, if their jurisdiction does not contain a local police department, the school district will then acquire, by federal law, a law enforcement officer who will assume the duties of an SRO at the next highest jurisdictional level; i.e., county, state, etc.

Schools are increasingly deploying armed personnel (Blanchfield, 2013). The presence of armed personnel allows for a quicker response to active shooters, whether the threat is from insiders or outsiders (Reyes, 2014).

The results of this study, as well the review of the policies and procedures of the New Jersey Department of Education and the policies and procedures of the NJDFG GH public school districts, can allow principals to possess a clearer vision of their role of being prepared for a shooter emergency.

I further believe that the New Jersey Suburban Public School Districts 1-8 (District Factor Group 'GH') should establish the following parameters in all districts of 'GH' that participated and otherwise noted:

• The training of teachers in identifying behavioral problems to be conducted by school principals

• The training of teachers to address troubled students and/or parents to be conducted by school principals

•The training of all staff on physical security operations

School principals should be monitored by their districts regarding their competence relevant to adhering to the protocol set forth by the New Jersey Attorney General, as it applies to the Model School Security Policies.

The New Jersey Suburban Police Departments 1-8 (Jurisdictional Agencies) should be mandated to do the following:

1. Police departments, through their liaisons, and consistent with the Memorandum of Agreement between Education and Law Enforcement Officials, should provide training to police officers specifically assigned to these schools in the identification of behavioral problems and understanding of troubled students and their parents;
the larger dilemma requires more than simply assigning a police officer to sit and wait for an armed intruder.

2. Police departments, through their liaisons and consistent with the Memorandum of Agreement between Education and Law Enforcement Officials, should notify the school district liaison of every shooting or homicide within these jurisdictions to ensure that the students that may or may not be affected by the incidents that occur are provided with necessary assistance.

3. Canine teams should be obtained and deployed, when necessary, in conjunction with

SRO training, as an available option to their department and the schools they protect, when confronted with active shooter scenarios, which may occur within suburban public schools in New Jersey.

Although they recognize that the problems affecting schools within a New Jersey suburban public school district may vary, I determined that approximately 14% (3) of the principals possessed either no knowledge of the magnitude in which active shooter scenarios occur within suburban school settings, or were in complete denial. Is a firearm the dominant resource to defend an attack inside a New Jersey suburban public school? Perhaps it is, if armed personnel possess the proper training to actually be considered "armed personnel" in an official capacity. Nonetheless, human error can occur in any case, whether holding a firearm to protect a child in a school, or failing to identify the individual who may need help the most, through the eyes of a closed-circuit camera, or the press of a button on a piece of advanced technology.

Recommendations for Future Study

This current study focused on topics that are critical to our nation, and vital to school safety and security. There is considerable room for further research. Possible directions of future research could include (1) revisiting the same suburban New Jersey District Factor Group 'GH', and interviewing teachers, rather than administrators as in this study; (2) sampling larger district factor groups, which could include even more affluent districts, as well as districts much lower in socioeconomic status, and schools with larger student populations than in this study or that by (Reyes, 2014); (3) conducting an analysis of student perceptions and experiences in regards to security.

My study had a small sample size, which could potentially be rectified in the future. Also, face-to-face interviews can elicit different kinds of information than anonymous surveys and questionnaires, which should be considered for future research.

References

1. Attorney General Law Enforcement Directive 2007-1 (2007, July 13). Retrieved from http://www.njdcj.org/agguide/directive/dir-le_dir-2007-1.pdf
2. Blanchfield, K., & Ladd, P. (2013). Leadership, violence, and school climate: Case studies in creating non-violent schools. Lanham, MD: Rowan and Littlefield Education.
3. Gun Violence Archive. (2016). Gun Violence Archive. Retrieved November 4, 2016, from www.gunviolencearchive.org.
4. Golgowski, N. (2015). "Father of Muslim teen arrested for clock previously battled Fla. Koran burner, has run for president of Sudan twice". Retrieved from http://www.nydailynews.com/news/national/father-muslim-kid-arrested-clock-standout-citizen-article-1.2363466
5. Holtz, L. E. (2014b). *Laws of arrest and seizure*. Woodbine, NJ: Holtz Learning Centers.
6. Jackson, A. (2002), "Police-school resource officers' and students' perception of the police and offending", *Policing: An International Journal of Police Strategies and Management* , Vol. 25 No. 3, pp. 631-650
7. Klein, J. (2005). Teaching her a lesson: Media misses boys' rage relating to girls in school shootings. Crime, Media, Culture, 1(1), 90-97. Kowalski, T. (2010). The school principal: Visionary leadership and competent management: 1st edition. New York, NY: Routledge.
8. Mittelman, W. (1991). Maslow's study of self-actualization: A reinterpretation. *Journal of Humanistic Psychology, 31*(1), 114–135.
9. New Jersey Department of Education. (2004, August 16). District factor groups. Retrieved from http://www.state.nj.us/education/finance/rda/dfg.html
10. New Jersey Department of Law and Public Safety and the New Jersey Department of Education. (2014). *A uniform state memorandum of agreement between education and law enforcement officials*. Retrieved from http://www.njus/education/schools/security/regs/agree.pdf
11. Reyes, R. (2014). School Shootings and Principals' Perception of Armed Personnel in an Education Setting.
12. State of New Jersey. (1998). *New Jersey school search policy manual*. Retrieved from http://www.state.nj.us/lps/dcj/school/school1.pdf
13. Ujifusa, A. (2012, December 20). Debate stirred on arming teachers, school staff. Education Week. Retrieved from http://www.edweek.org/ew/articles/2012/12/19/15newtown-arms.h32.html

How Productive are the DOE National Laboratories in Terms of Publishing and Patenting?*

Roger G. Johnston, Ph.D., CPP
Right Brain Sekurity

Abstract

This paper summarizes a rudimentary analysis of the publication and patent productivity of DOE National Laboratories. The work at these laboratories has significant implications for security.

Acronyms

Ames: DOE Ames Laboratory (Ames, IA)
ANL: Argonne National Laboratory (Lemont, IL)
BNL: Brookhaven National Laboratory (Upton, NY)
DOE: United States Department of Energy
FermiLab: Fermi National Accelerator Laboratory (Batavia, IL)
FOIA: Freedom of Information Act
FTE: Full-Time Equivalent Employee(s)
FY: Fiscal Year, generally starting October 1 for DOE laboratories
IAEA: International Atomic Energy Agency
INL: Idaho National Laboratory (Idaho Fall, ID)
NNSA: National Nuclear Security Administration
LANL: Los Alamos National Laboratory (Los Alamos, NM)
LBNL: Lawrence Berkeley National Laboratory (Berkeley, CA)
LDRD: Laboratory Directed Research and Development
LLNL: Lawrence Livermore National Laboratory (Livermore, CA)
MagLab: National High Magnetic Field Laboratory (Tallahassee,FL)
MDMP: Multidisciplinary, Multiprogram
NGO: Non-Government Organization
NREL: National Renewable Energy Laboratory (Golden, CO)
ORNL: Oak Ridge National Laboratory (Oak Ridge, TN)
PNNL: Pacific Northwest National Laboratory (Richland, WA)
PR: Public Relations
R&D: Research and Development
SLAC: Stanford National (Linear) Accelerator Laboratory (Stanford, CA)
SNL: Sandia National Laboratories (Albuquerque, NM)
SRNL: Savannah River National Laboratory
UCNI: Unclassified (but) Controlled Nuclear Information
U.S.: United States
Y-12: Y-12 nuclear complex (Oak Ridge, TN)

*This paper was not peer-reviewed.

Introduction

Depending on how you count them, there are about 17 "national" laboratories owned by the United States Department of Energy (DOE). Of these, 10 are typically considered large, multidisciplinary, multiple program (MDMP) labs: ANL, BNL, INL, LANL, LBNL, LLNL, ORNL, PNNL, SNL, and SRNL.

Three of these 10 labs (LANL, LLNL, SNL) are R&D nuclear weapons labs, and 2 are nuclear support labs (INL, SRNL). The DOE Office of Science manages the remaining 5 so-called science labs: ANL, BNL, LBNL, PNNL, and ORNL. In theory, these science labs, and to a lesser extent the 2 nuclear support labs are more devoted to R&D and to fundamental science/engineering research than the DOE weapons labs, and might be expected to publish and perhaps patent more. Despite the moniker "weapons labs", however, LANL, LLNL, and SNL actually do a great deal of R&D, plus government support and training services that are unrelated to weapons, nuclear technology, or classified projects.

DOE also owns the Ames, FermiLab, NREL, and SLAC national laboratories, as well as the Y-12 nuclear complex, and these were all considered in this study. For comparison, a non-DOE laboratory, MagLab was also included in this study.

All the DOE national labs, and particularly the 10 MDMP labs, have had—and continue to have—a significant impact on U.S. security. The DOE labs conduct R&D on a variety of nuclear, safeguards, nonproliferation, defense, national security, intelligence, counter-intelligence, and homeland security issues. They develop novel technologies and security strategies; provide technical advice to the federal government, the IAEA, and private industry; and (increasingly) provide (non-R&D) security support and training services to the government. Thus, the productivity of these laboratories is a matter of potential interest to this Journal's readership.

There appears to be relatively little in the way of recent, readily available, independent analysis or critiques of the productivity of the DOE national laboratories apart from specific

(and often harsh) criticisms by political activists or special interest NGOs, such as those devoted to environmental activism, nuclear nonproliferation/disarmament, the efficient use of taxpayer dollars, or countering the perceived mistreatment of laboratory employees. DOE and NNSA do internal contract evaluations of the labs, but these are not independent or widely distributed, and are (arguably) somewhat self-serving. There are also external scientific reviews of various laboratory Divisions, which often take place every 2-4 years; These may be accessible under FOIA but were not used in this study.

In 2015, the Commission to Review the Effectiveness of the National Energy (i.e., DOE) Laboratories completed its report.[1] Rather than being a technical productivity analysis of the DOE labs, this study largely focused on DOE management of the labs, strategic planning, duplication of capabilities, technology transfer, and LDRD programs. (The latter has long been a political football and hand-wringing obsession of Washington despite the relatively modest funds involved). Recent NGO reports [2,3] also focused more on DOE's management of the labs than on laboratory productivity *per se*.

In this, admittedly rudimentary study, I attempt to examine the productivity of the DOE laboratories by focusing on the number of public releases of documents, published papers, and issued patents. These are certainly not the only possible metrics for lab productivity, but they are relatively straightforward. Moreover—especially for the science labs—papers and patents are a primary product of R&D, and the main way that technical knowledge is widely shared. Even scientists and engineers who are engaged in more technical support than R&D often have technical discoveries, insights, viewpoints, and instrumentation that would merit sharing. Indeed, publishing and patenting are important for professional development, if nothing else. Even those engaged in classified work can generate unclassified reports, presentations, papers, and patents—as I have done frequently myself while working at ANL and LANL for a total of 31 years.

Ultimately, whether the DOE labs are making good use of taxpayers' money is a complex, value-judgment that I will not attempt to make here from these very limited results. This brief study, however, represents at least one look at the issue.

Results and Discussion

The data obtained for this study were found from online sources, as well as a single Freedom of Information Act (FOIA) Request that I submitted to DOE in June of 2016. This raw data appears in tables 1 and 2. Tables 3 and 4, as well as figures 1 and 2, show computed results based on the data in tables 1 and 2.

Table 1 - Data for 16 different laboratories.

Institution [References]	FTE Employees[a]	Ph.D.s[b]	Workforce[c]	Facility Users	Budget[d] ($ millions)
ANL [4]	3298		4070	7186	760
BNL [5]	2989		3388	4427	635
INL [6]	3900		4250		917
LANL [7]	6850	1450	8300	1200	2250
LBNL [8]	3395		3888	9300	680
LLNL [9]	6300	1090		700	1500
ORNL [10]	4368		4888	3115	1650
PNNL [11]	4400		5153	1996	900
SNL [12]	10540	1871	11405		2870
SRNL [13]	950				240
Ames DOE [14]	310	200			47
FermiLab [15]	1757			4300	360
MagLab [16]	743	282		1500	49
NREL [17]	1700		2000		358
SLAC [18]	1684		1800	3411	430
Y-12 [19]	4700				1187

a. Full-time equivalents, excluding contractors, students, post-docs, and visiting scientists.
b. Ph.D. employees only.
c. Workforce = FTE employees + postdocs + students, but does not include contractors, visiting scientists, or facility users.
d. Budget = average of the FY14 and FY15 budgets, or else an estimate based on other years.

A blank entry for a given cell in the tables indicates I was unable to obtain that information during the course of this (quite limited) study. Note that the number of public releases, publications, or peer-reviewed papers per Ph.D. in table 4 is the total number of such documents generated by the organization by any employee(s) divided by the number of Ph.D.'s in that organization. It is <u>not</u> the total number of such documents by Ph.D. authors divided by the number of Ph.D.'s in that organization. Similarly, the ratio of budget

to public releases and budget to number of patents are just the simple ratios, not the average actual cost of the work that went into each release or patent.

Table 2 - Additional Data for the 16 laboratories for 2014 and 2015.

Institution [References]	Public Releases 2014, 2015	Publications[a] 2014, 2015	Peer-Reviewed Papers 2014, 2015	Classified & UCNI Releases 2014, 2015	Patents Issued[b] 2014, 2015
ANL [4]	1754, 2286			0, 0	39, 63
BNL [5]	1659, 1236	1549, 1518		0, 0	21, 24
INL [6]	676, 451			1,2	24, 18
LANL [7]	1249, 1918			1, 2	34, 56
LBNL [8]	10558, 6272	3212, 3009	2719, 2747	0, 0	0, 1
LLNL [9]	1021, 724			1, 4	110, 92
ORNL [10]	2185, 1436			5, 20	79, 76
PNNL [11]	1666, 1357		1050, 1050	0, 0	57, 51
SNL [12]	2636, 2954			397, 0	108, 110
SRNL [13]	238, 305			0, 0	16, 17
Ames DOE [14]				0?. 0?	2?, 2?
FermiLab [15]	639, 673	345, 380		0?, 0?	2, 3
MagLab [16]	586, 573	461, ~441	238, 232	0?, 0?	5, 2
NREL [17]	1000			0?, 0?	35, 27
SLAC [18]	at least 850, 850	850, 850		0?, 0?	
Y-12 [19]	15, 9			36, 9	7, 0

a. Includes published books and papers, but excludes conference abstracts, PowerPoint presentations, and PR and training materials.
b. U.S. patents issued in 2014 and 2015 with the laboratory as the assignee. Does not include foreign or provisional patents.

It is probably useful to clarify the difference between the 3 categories of "publication". "Public Releases" involve a wide variety of materials that must—according to DOE regulations—be reviewed and logged prior to public release from a DOE national laboratory. This includes journal papers, books and book chapters, conference abstracts, PowerPoint presentations, conference proceedings, PR materials, public training and educational materials, etc. The category of "Publications" in my tables refers to a subset of "Public Releases" involving published technical papers, books, and book chapters. "Peer-Reviewed Publications" are a subset of "Publications" that get printed in journals that are peer-reviewed. Peer-reviewed papers are widely considered the publications of greatest quality, though that conclusion is not always warranted, and not all technical fields have equal access to peer-review publishing, including Physical Security.[20]

Table 3 - Computed ratios from data in tables 1 and 2.

Institution [References]	Public Releases[a] ÷ Employees	Publications[b] ÷ Employees	Annual Budget ÷ Public Releases[a] ($K)	Annual Budget ÷ Peer-Reviewed Publications[b] ($K)	Annual Budget ÷ Patents Issued[c] ($Million)
ANL [4]	0.61		380		14.9
BNL [5]	0.58	0.51	440		30
INL [6]	0.14		1600		44
LANL [7]	0.23		1400		50
LBNL [8]	2.49	0.92	81	250	1400
LLNL [9]	0.14		1700		14.9
ORNL [10]	0.41		910		21
PNNL [11]	0.34		600	860	17
SNL [12]	0.27		1030		26
SRNL[13]	0.20		880		14.5
Ames DOE[14]					24
FermiLab [15]	0.37	0.21	550		140
MagLab [16]	0.11	0.61	85	210	14.0
NREL [17]	0.60		360		12
SLAC [18]	at least 0.50	0.50	less than 510		
Y-12 [19]	0.01		99000		340

a. Public Releases per year averaged from 2014 and 2015 numbers.
b. Publications per year averaged from 2014 and 2015 numbers.
c. Computed using the number of U.S. issued patents per year for each lab, averaged from 2014 and 2015 numbers. The values shown in this column are simply the laboratory's annual budget divided by the number of annual issued patents (averaged for 2014 and 2015). This figure does not consider the actual cost of developing each individual patent, nor the fact that the majority of a laboratory's budget is not devoted to pursuing patents.

Table 4 - Additional computed ratios from data in tables 1-3.

Institution [References]	Public Releases ÷ Ph.D.s[a]	Publications ÷ Ph.D.s[a]	Peer–Reviewed Publications ÷ Ph.D.s[a]	Peer-Reviewed Publications ÷ Employees
ANL [4]				
BNL [5]				
INL [6]				
LANL [7]	1.09			
LBNL [8]				0.81
LLNL [9]	0.80			
ORNL [10]				
PNNL [11]				0.24
SNL [12]	1.49			
SRNL [13]				
Ames DOE [14]				
FermiLab [15]				
MagLab [16]	2.05	1.60	0.83	0.32
NREL [17]				
SLAC [18]				
Y-12 [19]				

a. This is a simple ratio, not the actual number of releases or publications per Ph.D. author.

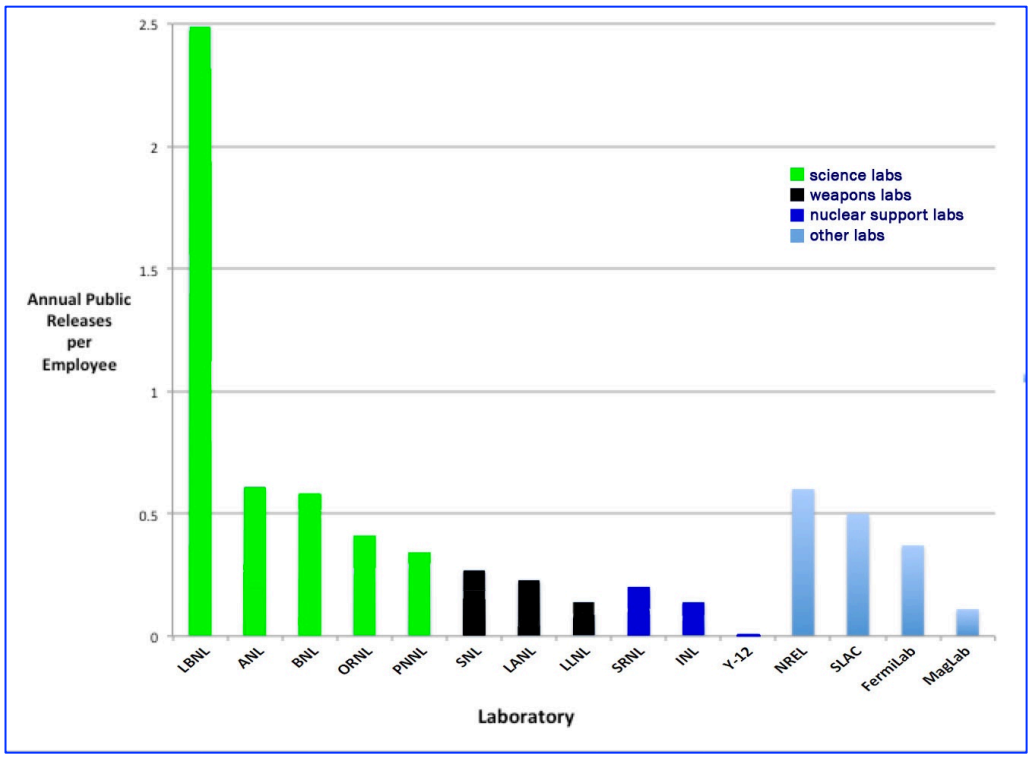

Figure 1 - Annual public releases per employee for various labs. The DOE science labs are green, weapons labs black, nuclear support labs dark blue, and other labs light blue. LBNL has the highest number of all the labs at 2.49 public releases per employee.

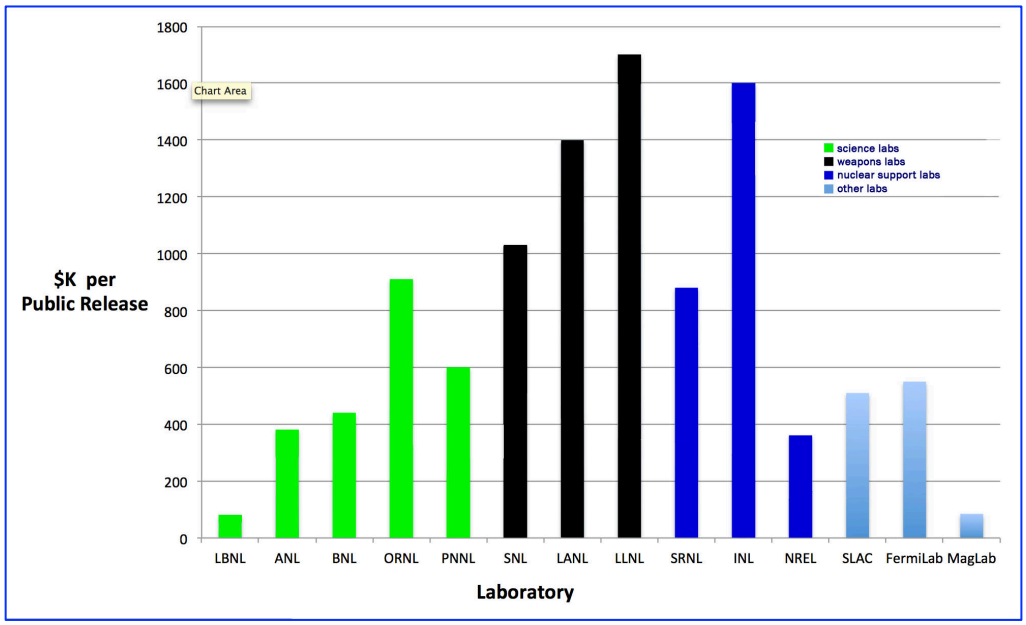

Figure 2 - $K of budget per public release for various labs. DOE science labs are green, weapons labs black, nuclear support labs dark blue, and other labs light blue. LBNL is the most cost-effective laboratory at $81K per public release.

To summarize the results in tables 3 and 4, and figures 1 and 2:

The top labs out of the 16 shown in table 3 in terms of public releases per employee were LBNL by a factor of 4 over second place ANL, followed by BNL, ORNL, and PNNL. Surprisingly, the 3 DOE R&D weapons labs (LANL, LLNL, and SNL) were only down about a factor of 2 from the DOE science labs in terms of public release per employee, despite doing much more classified work. The science laboratories, doing a lot of basic science and unclassified engineering, might reasonably have been expected to have a higher document output *vis a vis* the weapons labs.

The top labs in having the lowest cost per public release were the following: LBNL, again by a wide margin over other MDMP labs, followed by MagLab, NREL, SLAC, and FermiLab. Perhaps not surprisingly, the 3 DOE R&D weapons labs were much more expensive per public release than the DOE science labs.

The top labs in lowest cost per U.S patent issued: NREL, followed by MagLab, SRNL, LLNL, and ANL. The 3 DOE R&D weapons labs did quite well considering their mission, finishing in the middle of the pack.

Results for public releases per Ph.D., publications per Ph.D., and peer-reviewed publications per employee were spotty. The results that could be determined (table 4) show a remarkably low output. There are far fewer publications and peer-reviewed publications for these labs than would be expected as a minimum for a tenure-track professor in academia—at least 2-3 or more per year not counting non-peer-reviewed papers/books and conference presentations.[21] And university personnel often have a substantial teaching load with little analog in the national labs. Academic professors must also devote a considerable amount of time to advising students and to "service" responsibilities (committee duties) that far exceed those of technical staff members at DOE national labs, at least based on my experience at ANL and LANL, and many years of interacting with technical staff members at the other 8 DOE MDMP labs. On average, university faculty at large research universities spend an average of around 40% of their

time on research (counting weekends and summers).[22] This is much less in my experience than what is typical for technical staff members at DOE national labs by about a factor of 2. With more time and less non-R&D distractions (such as teaching and students), DOE laboratory scientists and engineers should have greater opportunities for publishing than their colleagues in academia.

The laboratories with extensive user facilities have many (non-employee) visitors who use lab facilities. These visitors are called "facility users". They should give laboratory employees extra opportunities for technical releases and papers (as well as fresh ideas). Now it is true that some facility users do proprietary work and don't publish. Many do, however, including for the reason that DOE does not charge fees if their work is meant to be openly published. DOE laboratory personnel should also have opportunities for publishing and giving conference presentations when they develop technologies, techniques, and instrumentation to make the facility user's measurements possible, quite independently of the users' publications. (Note that a publication by facility user would ordinarily not be counted as a DOE lab public release unless an employee of the laboratory was a co-author.)

The DOE labs with the greatest number of annual facility users were LBNL with 9,330 in 2016 [8]; ANL with more than 7,186 in 2015 [4]; BNL with 4,427 in 2016 [5]; FermiLab with 4,300 in 2016 [15]; and ORNL with 3,115 in 2016 [10]. Indeed, this is approximately the order they are in for Public Releases per Employee (figure 1). The linear correlation coefficient for number of Public Releases per Employee (table 3, column 2) versus the number of annual Facility Users (table 1, column 5) for the 11 labs in Table A with full data is r=0.84. This indicates that document production (and presumably publication) is strongly correlated with the number of facility users—even though the facility users publications aren't counted as DOE lab Public Releases.

Problems and Limitations of This Work

Neither DOE or the individual DOE labs provided all the records requested in my (fairly modest) FOIA request. FermiLab claimed not to keep records of some of the data I requested, even though I later found the same information on the FermiLab websites, without having to run a search internally on those web pages.

Now there are many ways to measure productivity. This study focus on just one: document, publication, and patent output. Moreover, this study is a largely cursory analysis, but at least it is a start. It certainly would have been interesting to compare in detail DOE laboratory publication and patent quality, as well at the rate of citation versus other laboratories and compared with science and engineering departments in major U.S. research universities. After all, quantity is not quality—though quantity sometimes increases the opportunity for quality.

One of the problems of this study is that "Public Releases" are a mixed-bag of documents, not just technical papers and book chapters. Fortunately, the DOE MDMP labs are required to follow very similar DOE regulations and procedures in regards to formally reviewing and logging public releases, so the mixed-bag of public releases are probably quite similar. This might not be the case, however, for the non-MDMP labs, or for MagLab.

Another possible problem is that there was considerable anecdotal evidence when I worked at ANL that not all public releases were officially reviewed and would therefore not necessarily show up on the official list of public releases. This would be a violation of DOE regulations, but may well have occurred (and may continue to occur). If there are such documents, the majority would probably be conference abstracts, student posters and presentations, PR and training materials, major website updates, or essays from senior managers, but probably would include few technical papers. Thus, "Public Releases" for Argonne, and perhaps some of the other non-weapons labs may be underreported. In contrast, at LANL, I saw little evidence of such practices, which is probably to be expected given that classification is a bigger issue at the DOE weapons labs.

The analysis of the number of patents has its own limitations. Patents are certainly some measure of innovation, but the fact is that most patents are worthless.[23] Moreover, patents are mostly old news; they represent past work. Patents are typically issued 2-5 years after filing, and are based on work that often took place 4-8 years prior to the patent being granted. Provisional patents and non-U.S. patents (the latter rare for DOE labs) could also be considered but were not analyzed in this study.

Note also that I did not consider the number of (non-employee) contractors working at each lab. Increasing amounts of the work at the DOE labs, especially support, training, security, or environmental remediation work (in contrast to true R&D) seems to be being done by contractors. (Many projects called "R&D" by DOE and/or the national labs cannot reasonably be considered R&D.) Another issue is that the different laboratories might also have somewhat different definitions for "facility users".

Another problem is that some of the figures in the tables are estimates for the averages for 2014 and 2015, yet taken from different years.

Still another problem occurs with trying to include Y-12 (and possible SRNL) in this analysis. As DOE pointed out (unsolicited and rather defensively) in its FOIA response, "the Y-12 National Security Complex is a manufacturing facility that does not typically issue technical publications." While one should certainly not expect Y-12 personnel to publish or patent at the same rate as R&D labs, the very low production is still surprising for reasons discussed above.

Conclusion

Of all the labs, LBNL, NREL, and MagLab seem to be the most efficient and productive in terms of generating publications and patents. Generally the output of the other DOE labs—at least as measured by public releases, publications, and patents—was disappointing. The

relatively weak performance of the DOE MDMP labs—not dramatically better than the R&D weapons labs with far fewer opportunities to publish—was also disheartening. This is especially true given the large number of facility users that visit the non-weapons labs, providing extra opportunities for public releases, publications, and patents.

Clearly, independent and more rigorous analysis of the technical productivity of the DOE labs is in order.

Notes and References

1. "Final Report to Review the Effectiveness of the National Energy Laboratories", (2015), https://energy.gov/labcommission/downloads/final-report-commission-review-effectiveness-national-energy-laboratories.

2. National Academy of Public Administrators, "Positioning DOE's Labs for the Future: A Review of DOE's Management and Oversight of the National Laboratories" (2015), http://www.lasg.org/documents/NAPA_2Jan2013.pdf.

3. National Research Council, "Managing for High-Quality Science and Engineering at the NNSA National Security Laboratories" (2011), https://www.nap.edu/catalog/13367/managing-for-high-quality-science-and-engineering-at-the-nnsa-national-security-laboratories

4. ANL Data:
"Labs-at-a-Glance: Argonne National Laboratory", http://science.energy.gov/laboratories/argonne-national-laboratory/. For 2016?: 3,402 full time employees, 812 students.
"About Argonne", https://www.anl.gov/about-argonne. For 2015: Budget: $760 million; 3,298 FTEs, 315 postdocs, 457 grad and undergrad students; 7,186+ facility users.
Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 1,754 in 2014 and 2,286 in 2015. Classified & UCNI releases in 2014 and 2015: 0 and 0.
U.S. Patent Office search for U.S. patents issued for 2014 and 2015: 39 and 63.

5. BNL Data:
"Labs-at-a-Glance: Brookhaven National Laboratory", http://science.energy.gov/laboratories/brookhaven-national-laboratory/. In 2016?: 2,989 full time employees, 399 students; budget $635; 4,427 facility users.
Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 1,659 in 2014 and 1,236 in 2015. Classified & UCNI releases in 2014 and

2015: 0 and 0.

Public releases, publications, and patents issued according to a BNL response to the RG Johnston DOE FOIA Request of June 25, 2016: Journal Articles: 1,549 and 1,518 in 2014 and 215; Full text releases (non-publications): 1 and 411 in 2014 and 2015; 21 and 26 patents issued in 2014 and 2015.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Brookhaven Science Associates, LLC): 21 and 24.

6. INL Data:

"The Nation's Nuclear Energy Laboratory", https://www.inl.gov/about-inl/general-information/. 3,900 employees and more than 350 "interns". In 2015, the budget was $917.1 million.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 676 in 2014 and 451 in 2015. Classified & UCNI releases in 2014 and 2015: 0 and 0.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Battelle Energy Alliance, LLC): 24, 18.

7. LANL Data:

"LANL Facts and Figures", http://www.lanl.gov/about/facts-figures. In 2016: 6,850 employees (21% of LANS employees + students have Ph.D.s), 350 postdocs, 1,100 students.

"LANL Budget", http://www.lanl.gov/about/facts-figures/budget.php. Budget for 2016: $2.45 billion.

"LANL User Facilities", http://www.lanl.gov/collaboration/user-facilities/index.php. More than 1,200 facility users per year.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 1,249 in 2014 and 1,918 in 2015. Classified & UCNI releases in 2014 and 2015: 1 and 2.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Los Alamos National Security, LLC): 34 and 56.

8. LBNL Data:

"Labs-at-a-Glance: Lawrence Berkeley National Laboratory, http://science.energy.gov/laboratories/lawrence-berkeley-national-laboratory/. In 2016, 3395 full time employees, 493 students; budget $683 million; 9,330 facility users.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 10,558 in 2014 and 6,272 in 2015. Classified publications: 0 in 2014; 0 in 2015.

Papers published according to a LBNL response to the RG Johnston DOE FOIA Request of June 25, 2016: 3212 in 2014 and 3009 in 2015.

Papers published in peer-reviewed journals according to a LBNL response to the RG Johnston DOE FOIA Request of June 25, 2016: 2719 in 2014 and 2747 in 2015.

—U.S. Patent Office search for U.S. patents issues for 2014 and 2015: 0 and 1.

9. LLNL Data:

"Lawrence Livermore National Laboratory: About", https://www.llnl.gov/about. 6,300

employees (including term employees and post-doctoral fellows); 2,700 scientists and engineers (more than 40% of whom are Ph.D.s); FY13 fiscal year budget $1.5 billion; 700 facility users.

"Lawrence Livermore National Laboratory", https://en.wikipedia.org/wiki/Lawrence_Livermore_National_Laboratory. Staff of 5,800. Budget of $1.5 million.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 1,021 in 2014 and 724 in 2015. Classified & UCNI releases in 2014 and 2015: 1 and 4.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015: 110 and 92.

10. ORNL Data:

"Oak Ridge National Laboratory", https://www.ornl.gov/content/frequently-asked-questions. Budget in 2016?: $1.65 billion.

"Labs-at-a-Glance: Oak Ridge National Laboratory", http://science.energy.gov/laboratories/oak-ridge-national-laboratory/. In 2016?: 4,368 full time employees, 520 students; 3,115 facility users.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 2,185 in 2014 and 1,436 in 2015. Classified & UCNI releases in 2014 and 2015: 5 and 20.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: UT-*BATTELLE,* LLC (*Oak* Ridge, TN)): 79 and 76.

11. PNNL Data:

"About PNNL", http://www.pnnl.gov/about/facts.asp. In 2016: 1,058 peer-reviewed published articles; over 4,400 employees; $920 million budget, 104 patents.

"Labs-at-a-Glance: Pacific Northwest National Laboratory", http://science.energy.gov/laboratories/pacific-northwest-national-laboratory/. For 2016?: 4,100 full time employees, 753 students, 1,996 facility users.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 1,666 in 2014 and 1,357 in 2015. Classified & UCNI releases in 2014 and 2015: 0 and 0.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Battelle Memorial Institute (Richland, WA)): 57 and 51.

12. SNL Data:

"Sandia National Laboratory by the Numbers", http://www.sandia.gov/news/publications/fact_sheets/_assets/documents/SNL_Numbers_Overview_FS_2016-1403.pdf. 10,540 regular employees in 2016, with 1871 doctorates. 187 postdocs and 678 students.

"Sandia National Laboratories: Facts and Figures", http://www.sandia.gov/about/facts_figures/. 2016 budget was $3070 million; 10,652 regular employees, 223 postdocs, and 738 students; 1857 doctorates.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 2,636 in 2014 and 2,954 in 2015. Classified & UCNI releases in 2014 and 2015: 397 and 0.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Sandia Corporation (*Albuquerque, NM*)): 108 and 110.

13. SRNL Data:

"Savannah River National Laboratory", https://en.wikipedia.org/wiki/Savannah_River_National_Laboratory. In 2010: 945 employees, $210 million budget.

Public releases according to a DOE response to the RG Johnston DOE FOIA Request of June 25, 2016: 238 in 2014 and 305 in 2015. Classified & UCNI releases in 2014 and 2015: 0 and 0.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Savannah River Nuclear Solutions, LLC): 16 and 17.

14. Ames DOE Lab Data:

"Labs-at-a-Glance: Ames Laboratory", http://science.energy.gov/laboratories/ames-laboratory/. For 2016?: 310 full time employees and 149 students; budget $47 million.

"Ames Lab at a Glance", https://www.ameslab.gov/about/ames-lab-at-a-glance.

The estimated number of patents is about 2 each year based on "Iowa State Universit450 employees, 260 scientists.

Digital Repository", http://lib.dr.iastate.edu/ameslab_patents/ and "Ames Laboratory: Intellectual Property, Patenting and Licensing ", https://www.ameslab.gov/techtransfer/intellectual-property-patenting-and-licensing. (Note that the Iowa State University Foundation that runs the Ames Laboratory is the assignee on a number of patents not part of the Ames DOE laboratory.)

15. Fermi Lab Data:

"Fermilab", https://en.wikipedia.org/wiki/Fermilab. $345 million annual budget. "Lab-at-a-Glance: Fermi National Accelerator Laboratory", http://science.energy.gov/laboratories/fermi-national-accelerator-laboratory/. For 2016?: 1757 full time employees, $371 million annual budget; 4,300 facility users.

"FermiLab Research at a Glance", http://ccd.fnal.gov/techpubs/fermilab_research_glance.html. 2014, 2015 releases: 639, 673. 2014, 2015 papers: 345, 380.

U.S. Patent Office search for patents issued for 2014 and 2015 (Assignee: Fermi Research Alliance, LLD): 2, 3.

16. MagLab Data:

"National High Magnetic Field Laboratory 2014 Annual Report", https://nationalmaglab.org/images/research/publications/searchable_docs/annual_reports/AReport_2014_web.pdf. 452 user reports in 2014. 450 papers published in peer-reviewed journals in 2014 but this may involve more authorship by users than by MagLab staff. 11 books, book chapters, and reviews in 2014. MagLab staff conducted over 360 conference presentations and 5 workshops/conferences. Budget in 2014 was $48.4 million.

"MagLab By the Numbers", https://nationalmaglab.org/about/facts-figures/by-the-numbers. (Presumably 2014 figures.) 743 employees. 38% (282) have Ph.Ds. $48.4 million budget. 1,500 facility users per year.

"MagLab Peer-Reviewed Publications", https://nationalmaglab.org/research/publications-all/peer-reviewed-publications. 238 and 232 peer-reviewed publications in 2014 and 2015, respectively.

"MagLab Publication Search", https://nationalmaglab.org/research/publications-all/publications-search. A search for 2014: 29x20+6=586. Journals only is 22x20+9=449. Books is 12. 5 patents. A search for 2015: 28x20+13=573 (includes theses and dissertations). Journals only is 21x20+9=429. Books only is 8x20+17=177. 2 patents. Note that 2014 and 2015 presentations are not publications, so that the numbers entered in the publications column in table 2 may be too low for MagLab.

17. NREL Data:

"NREL Recent Funding", http://www.nrel.gov/about/funding-history.html. $360 million in 2014 and $357 million in 2015.

"Transforming Energy Through Science", http://www.nrel.gov/docs/fy16osti/66385.pdf ~1700 full and part-time employees, 314 postdocs and students, >1000 publications per year.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Alliance for Sustainable Energy, LLC): 35 and 27.

18. SLAC Data:

"Lab at a Glance", http://science.energy.gov/laboratories/slac-national-accelerator-laboratory/. 1684 full time employees, 124 students, 3,411 facility users.

"SLAC + Stanford", https://www6.slac.stanford.edu/files/SLAC_Stanford_report_2016_final.pdf. Annual budget $433 in 2015.

"SLAC", https://www.drupal.org/node/2707401. 850 research papers a year.

19. Y-12 Data:

"Y-12 National Security Complex", https://en.wikipedia.org/wiki/Y12_National_Security_Complex. 4700 employees.

"NNSA 2016-2020 Congressional Budget Request" , https://nnsa.energy.gov/sites/default/files/nnsa/inlinefiles/NNSA%20FY%202016%20Budget%20Rollout.pdf. FY14 budget: $1187 million.

RG Johnston June 25, 2016 FOIA Request Response: 2014 and 2015 unclassified public releases = 15 and 9, respectively. 2014 and 2015 classified and UCNI releases = 36 and 9, respectively.

U.S. Patent Office search for U.S. patents issued for 2014 and 2015 (Assignee: Babcock & Wilcox Technical Services, Y-12, LLC): 7, 0.

20. RG Johnston and JS Warner, "Is Physical Security a Real Field?", Journal of Physical Security **7**(3), 13-15, (2014), http://jps.rbsekurity.com.

21. 2-3 peer-reviewed papers per year in tenure track seems to be a common MINIMUM number at a major research university but some people think 3-5 is the minimum number, depending on the field and whether experimental or theoretical, etc. See, for example, "Female Science Professor: Magic Number", http://science-professor.blogspot.com/2010/02/magic-number.html; J Blair, "The Publication Imperative", https://www.newscientist.com/article/dn21738-the-publication-imperative/ and Y Gingras, V Larivière, B Macaluso, J-P Robitaille (2008), "The Effects of Aging on Researchers' Publication and Citation Patterns", PLoS ONE 3(12): http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0004048

22. See, for example, "The Long, Lonely Job of Homo academicus", https://theblue review.org/faculty-time-allocation/; "Research, Teaching Dominate Professors' Time", http://www.browndailyherald.com/2011/10/24/teaching-research-dominate-professors-time/; G Fallis, *Rethinking Higher Education: Participation, Research, and Differentiation* (2014).

23. "Are Most Patents Useless?", https://www.quora.com/Are-most-patents-useless.