SANDIA REPORT
SAND2017-7995
Unclassified Unlimited Release
Printed July 2017

Two-Person Control
A Brief History and Modern Industry Practices

Robert D. Pedersen, MCJ

Sandia National Laboratories, Livermore, California

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Issued by Sandia National Laboratories, operated for the United States Department of Energy by National Technology and Engineering Solutions of Sandia, LLC.

Available to DOE and DOE contractors from
U.S. Department of Energy
Office of Scientific and Technical Information
P.O. Box 62
Oak Ridge, TN 37831

Telephone: (865) 576-8401
Facsimile: (865) 576-5728
E-Mail: reports@adonis.osti.gov
Online ordering: http://www.osti.gov/bridge

Available to the public from
U.S. Department of Commerce
National Technical Information Service
5285 Port Royal Rd.
Springfield, VA 22161

Telephone: (800) 553-6847
Facsimile: (703) 605-6900
E-Mail: orders@ntis.fedworld.gov
Online order: http://www.ntis.gov/help/ordermethods.asp?loc=7-4-0#online

SAND2017-7995
Unlimited Release
Printed July 2017

Two Person Control:
A Brief History and Modern Industry Practices

Robert D. Pedersen, MCJ
Security Operations and Emergency Management
Sandia National Laboratories
P.O. Box 969
Livermore, California 94550

Abstract

Physical asset protection is the principal objective of many security and safeguard measures. One well-known means of asset protection is two-person control. This paper reviews literature regarding two-person control to gain insight into its origin, first demonstrated uses, and its presence in several modern industries. This literature review of two-person control is intended to benefit people and organizations with a desire to understand its origins and how the practice has evolved over time, as well as give some insight into the flexibility of this safeguarding technique. The literature review is focused in four main sections: (1) defining two-person control, (2) early history, (3) two-person control in modern industry, and (4) a theory on how two-person control entered modern industry.

ACKNOWLEDGEMENTS

The author would like to thank Jarret Lafleur and Scott Paap of Sandia National Laboratories, California's Systems Analysis & Engineering organization for the opportunity to work on this project. Jarret Lafleur provided very constructive and helpful feedback through all stages of the work. Amanda Thompson of the Sandia California Technical Library maintained a great spirit and always had a quick document turnaround that very much helped out this project's completion.

Additionally, yet perhaps most importantly, the author would like to thank his wife and daughter, along with the rest of his family, for continued support over the years.

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

Considering two-person control, the image of two military members sitting next to each other turning keys simultaneously to launch a nuclear-armed missile is one ingrained in the American mind. This is an image crafted and refined by Hollywood movie and television producers wanting to bring tense drama to their viewers. Viewers are made to believe that these two people, purely products of circumstances, are now together burdened with the weight of the world in their next action of turning a launch key. Two-person control is more complicated than this image would suggest, however. More elements exist in two-person control than simply two arbitrary actors burdened with a fateful decision, as will be demonstrated. The history surrounding two-person control does not have such dramatic origins. In fact, two-person control for securing an asset originated from an unrelated industry more focused on financial asset protection and liability mitigation than on releasing a nuclear payload.

This paper reviews the history surrounding two-person control and the system's application in modern industries. Old journals, news stories, legal decisions, law reviews and committee proceedings help to form a picture of the practice over more than a century's timespan. Internal documents, news stories, academic studies and organizational reports help identify many industries that make use of two-person control. To present this literature review, the paper is divided into four main sections: (1) defining two-person control, (2) early history, (3) two-person control in modern industry and (4) a theory on how two-person control entered modern industry.

The reader will gain from this literature review an understanding of substantial portions of the history surrounding two-person control and examples of how it is practiced in modern industries. Examples of its practice range from physical to digital examples.

1. INTRODUCTION

Not long after 6:30 AM on November 26, 1983, six armed, masked men entered a warehouse near Heathrow Airport. Their target was a Brink's-Mat facility holding £3 million in cash, over forty pounds of platinum, one-thousand carats of diamonds and £26 million of gold destined for Hong Kong (Figure 1). The men physically attacked security guards on-site, even pouring liquid accelerant over the only two guards who had the keys and combinations to the Brink's-Mat vault to coerce them to provide the keys and combination to the vault containing £26 million in gold, platinum and diamonds. One can only imagine the thoughts running through the guards' minds. Threatened with their lives, the guards gave in and the robbers left with three tons of gold bars packed in 76 boxes and two boxes of diamonds.[1-4]

As it turned out, one of the Brink's-Mat employees playing victim during the robbery was an insider who willingly provided resources and information to the robbers that allowed them to circumvent security measures and defeat the established two-person control safeguards in place: a key to the warehouse's front door, alarm system information, and the identity of the two guards who each knew a portion of the vault combination and held keys to the vault.[1-3]

Figure 1. Police securing the scene of the Brink's-Mat facility[5]

The Northern Bank of Belfast fell victim to an even more intricately planned robbery involving hostage-taking, kidnapping and impersonation over the two days of December 19-20, 2004. Three unknown assailants went to a private residence outside of Belfast, Northern Ireland, on the night of December 19. Two of these men held the family of Chris Ward, a bank official with the Northern Bank of Belfast, while the third man kidnapped Ward and drove him south to County Down.[6-8]

In County Down, the assailants took Ward to the home of Kevin McMullan, Ward's work supervisor, where another group of assailants had already taken control of McMullan's house after impersonating police officers. The assailants kidnapped McMullan's wife and gave both Ward and McMullan instructions to assist in a bank robbery at the Northern Bank of Belfast the following day, December 20. Ward recalled that the assailants hinted at murdering his family if Ward and McMullan's participation in the robbery did not go as instructed. Ward and McMullan, not knowing the status of their families, agreed to execute the robbery.[6-8]

On Monday, December 20, both Ward and McMullan went to the bank. Both men possessed keys to the vault, granting them easy access. Ward and McMullan worked until the bank closed and other employees left at 6pm. Alone now, they let the criminals into the bank to steal the rest of the currency over the course of two hours (Figure 2). The thieves ultimately made off with £26.5 million in currency.[6-8]

Figure 2. Chris Ward leaving the Northern Bank with a gym bag full of cash[9]

What do the Brink's-Mat and Northern Bank thefts have in common? In both cases, determined actors coerced multiple personnel trained and charged with safeguarding physical assets. In the case of the Northern Bank robbery, bank employees held keys to a vault. In the case of the Brink's-Mat robbery, two workforce personnel safeguarded physical assets as separate individuals knowing the independent combinations required to access the asset, a clear example of a method known as two-person control. In both cases, criminals isolated specific personnel because those personnel had the means to access a high-value physical asset. Once isolated, the criminals successfully coerced the employees under threat of physical harm to the employees or their loved ones.

These examples demonstrate troubling instances of successful coercion to drive multiple responsible security personnel to collude and defeat their own security protocols. Yet two- or multi- person control is often understood as a measure to minimize the threat of collusion among insiders. This drives a number of critical questions: Against what types of threats does two-person control protect, and against what types of threats does it not? Have these two distinct sets of threats been widely understood, and for how long? Were the strengths and limitations of two-person control obvious from early in its history, and were they central considerations in its development or intended applications? How has the practice changed over time, and how is it utilized today? To begin laying a foundation for answering the former two questions, this report is a first step at addressing the latter two questions.

This report is organized as follows:

- Section 1 introduces two-person control through two real-life instances in which it was defeated.
- Section 2 defines identified elements of two-person control.
- Section 3 explores the early history of two-person control.
- Section 4 discusses two-person control as used in modern industries.
- Section 5 presents a theory on how two-person control evolved into so many modern industries.
- Section 6 provides a conclusion to this literature review.

2. ELEMENTS OF TWO PERSON CONTROL

One popular method in use today to minimize an organization's exposure to a criminal attack is two-person control. The concept of two-person control is that no one person is able to unilaterally access a physical asset. This concept is not foolproof, however, as demonstrated by the Brink's-Mat robbery.

Two-person control is widely known and implemented today in a variety of industries, as will be reviewed later in this paper. Identifying the elements of two-person control involves answering at least three distinct questions:

1) ***What is the threat (to my asset)?***

   A basic threat to any high-value asset is found by determining who wants the asset. One's perception of an asset's intrinsic value more accurately defines the threat than simply how much an item is worth monetarily. In other words, not everybody values assets using similar criteria. Petty thieves, organized criminal enterprises, terrorist organizations, and nation-states each value an asset differently. For example, a petty thief will not dedicate, or have access to, the same resources as that of a nation-state in order to access an asset. Rather, a petty thief will primarily have burglary tools and more crude social engineering techniques to gain access to an asset, whereas a nation-state has time, financing and national resources at its disposal. Similarly, a nation-state will not dedicate national resources in order to commit petty theft. An important point to remember is that outsiders to an organization with an asset are not the only people wanting the asset. Insiders can present just as much of a threat to an asset as outsiders.

2) ***How do I design my two-person control around that threat?***

   Implementation, as described here, includes both engineered and human (including administrative) implementation. Engineered implementation embodies hardware and software devices designed to make circumvention of two-person control difficult or nearly impossible. An example of engineered implementation includes vaults or safes requiring multiple locks or combinations to open. Human implementation includes procedural or administrative steps whose enforcement depends solely or primarily on human practice. An example of human implementation includes a responsible party required to unlock a safe with a key or combination only he or she possesses, while in conjunction a similar unlocking process is performed by a separate party. Human implementation of two-person control typically formalizes the fact that the two parties are acting concurrently with each another regarding the action being performed.

3) ***How do I know my two-person control practitioners are protecting their access from improper use?***

   Practitioners of two-person control implementations must safeguard their own access to an asset by ensuring that one person cannot unilaterally access an asset. Willfully or accidently providing access information, such as one's sequence for a vault combination, to someone with no need to know compromises safeguarding procedures. In many cases, an organization's policies or regulations require two-person control practitioners to take care that they do not divulge engineered or human implementations protecting an asset to anybody without a need to know, establishing grounds for some form of punishment for the practitioner not abiding by organizational policies or regulations. One emphasized practice to minimize instances of rule-breaking is to ensure employee reliability, which serves as an indicator of one's susceptibility to a range of incidents that could negatively impact two-person control safeguarding measures. As

will be reviewed, methods of ensuring employee reliability range from checking one's employment history to mental health history to a full-scale investigation into one's employment, mental health, criminal, social and financial history. The end result of these efforts is for an organization to prevent the compromise of the two-person control practitioner.

Stemming from an emphasis on employee reliability comes an almost rhetorical question that embodies a strategic concern: Quis custodiet ipsos custodes? Roughly translated from Latin, "Who will guard the guardians?" Ensuring that two-person control practitioners are reliable requires a vetting process that has to be vetted by someone else, which begs the question: Who is charged with ensuring that the person vetting two-person control practitioners is him- or herself reliable?* One finds that this line of questioning can quickly shift the burden of asset protection to focusing on employee reliability to an infinite degree. One must consider, however, both the benefits and concerns that come with shifting the burden of safeguarding an asset to focusing on employee reliability in order to design the best safeguarding solution for an asset protected by two-person control practitioners.

What methods does an organization employ to ensure a new hire will safeguard an asset even when the employee lacks associating factors capable of obvious compromise, such as personal financial instability or associations with criminal elements? For example, an organization could hire someone with a strong work ethic, demonstrated sense of honesty and integrity, with no financial issues or social connections that could otherwise expose that person to easy coercion. Consider the Brink's-Mat Heist and Northern Bank of Belfast robbery: The employees were trusted with access to an asset and did nothing malicious, but still found themselves coerced by extraordinary means that led to the robbery of an asset.† Are there identified practices that ensure that a two-person control practitioner is incapable, or at least less prone, to this type of extraordinary coercion?

Using the above elements, this paper will review the documented history of two-person control, from its earliest documented forms to the beginnings of its implementation as an industrial best practice. Following this history review, this paper will review literature documenting two-person control implemented through industry today.

* "Quis custodeit ipsos custodes custodum? – Who will guard the guardians of the guardians? Add "custodum" to the n^{th} degree of concern: Who will guard the guardians of the guardians of the guardians, etc.

† With the possible exception of Chris Ward, who, as mentioned in the previous section, was arrested for, but found not guilty of, conspiring to commit the Northern Bank of Belfast robbery.

3. EARLY HISTORY OF TWO-PERSON CONTROL

The core concept of two-person control, that an asset is more effectively safeguarded under the joint protection of peers rather than under the watch of an individual, has origins long before its employment in security systems. Elementary school students in the United States are well aware of this principle's implementation in the United States Constitution, ratified in 1788, which divided federal power between three separate branches of one federal government. In defense of dividing power between separate branches of government, James Madison, writing anonymously as Publius in February 1788, stated, "But the great security against a gradual concentration of the several powers in the same department, consists in giving to those who administer each department the necessary constitutional means and personal motives to resist encroachment of the others. The provisions for defence must in this, as in all other cases, be made commensurate to the danger of attack. Ambition must be made to counteract ambition."[10] Madison's argument was part of Federalist No. 51, one of many essays known as the The Federalist Papers that were written to rally support for the new United States Constitution.

The concept of two-person control is much older than the United States, however. The concept precedes the Magna Carta (Figure 3), initially chartered in 1215, which provided protection and recourse to the English populace from many arbitrary actions of an autocrat.

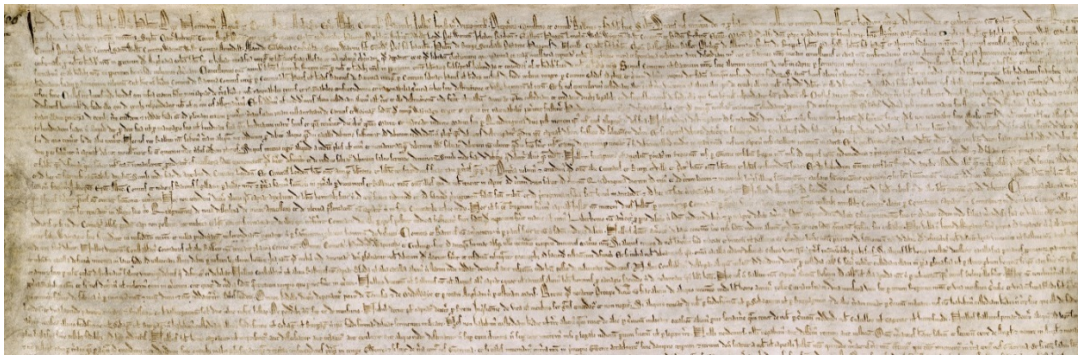

Figure 3. The Magna Carta[11]

Vesting powers from a single entity into multiple is a concept spanning over two-thousand years to at least the earliest years of the Roman Republic. Following the fourth-century B.C. revolution that created the early Roman Republic, Roman citizens elected two chief executives, called praetors‡, as opposed to one chief executive to rule as a single entity. As Frank Abbott notes in his 1901 work on Roman political institutions, "the participation of a colleague in the exercise of supreme power will tend to prevent a magistrate from becoming autocratic."[12] This passage embodies Madison's argument from the Federalist No. 51.

Over centuries of Roman expansion and the resulting need to enforce Roman laws hundreds if not thousands of miles away from Rome, the number and duties of praetors expanded.[12] Praetors began to individually rule Roman conquests, such as Spain, lead armies in Rome's name, as well as head courts adjudicating individual topics. For example, Cicero, one of the most influential orators in the Western world to this day, served as praetor for the extortion court in Rome in 66 B.C.[13] Interestingly enough, the usurpers of the Roman Republic who established the Roman Empire were sons of praetors: Julius Caesar, son of Gaius Julius Caesar, and Caesar Augustus, son of Gaius Octavius. Both Julius Caesar and Caesar Augustus colluded with others to form triumvirates, groups of three who controlled Roman affairs.§

‡ Not to be confused with the Roman Republic's later duplicate use of 'praetor,' bestowing upon the receiver a military command, such as the praetorship held by Julius Caesar prior to his becoming permanent dictator.

This thought of preventing unilateral action in the name of a political entity carried on over the centuries to manifest in philosophical treatises, such as Jean-Jacques Rousseau's *The Social Contract* in 1762 and foundational government documents, as noted above with the Constitution of the United States and the English Magna Carta.

The history surrounding two-person control for asset protection, though, is not as clearly documented. On two-person control, a security researcher wrote that, "The idea dates back to the days of the Cold War, where two operators were required, typically with two separate keys, for drastic action such as launching nuclear weapons."(14) A military research paper on biosecurity promulgates that notion by stating that it derives "from the chemical and nuclear programs and specifies that material is handled by two people of equal experience, training and qualification."(15)

A government document published by the United States Computer Emergency Readiness Team (US-CERT) defines the "two-person rule" as one in which "two people must participate in a task for it to be executed successfully."(16) The document continues to state that an example would "include requiring two bank officials to sign large cashier's checks."(16) This is not an especially fulfilling definition, though, as this explanation fails to specify what the act of two bankers signing a check actually serves to protect.

The clearest historical examples found as a result of this literature review regarding two-person control are historical accounts, legal decisions, and documents regarding concepts, rules and regulations of asset protection.

As stated above, two-person control, as we understand it, relies on a threat to a high-value asset, implementing the practice of two-person control and preventing human compromise. Each of these topics will now be reviewed.

3.1 Threat to an Asset

Financial industry literature demonstrates several instances in the late nineteenth and early twentieth centuries where the concept of two-person control is hinted upon, but not clearly defined. As will be demonstrated in the following section, the threat to an asset was identified as a safeguarding consideration to prevent both insiders and outsiders from improperly accessing an asset through the use of safe deposit boxes. The following literature provides some insight into how the financial industry began to form an industry standard of safeguarding safe deposit boxes (Figure 4).

Safe deposit boxes have been used as a customer-facing service in the United States since at least the 1860s. This safeguarding method allowed several parties to store items in individual metal boxes secured by a lock. One could imagine an apartment complex's mail box station serving several units (Figure 4). The Safe Deposit Company of New York, the United States' first safe deposit company in 1865, advertised the ability to rent five-hundred secured boxes, "'with renters having complete control of their individual box.'"(17) Even today, the practice of renting out safe deposit boxes is still a common practice in banking.

---

§ The First and Second Triumvirates ultimately betrayed one another, leaving Julius Caesar and Caesar Augustus to rule unilaterally following their respective Triumvirates, thus dissolving the Roman Republic and establishing the Roman Empire. Still, it is worth mentioning that the precedent of three-person rule is evident in such instances as the United States Constitution that separates powers among three branches of government. Further, one of these branches is still divided between two separate Houses of the United States Congress: The House of Representatives and the United States Senate, each of which have their own specific methods to check and balance the other.

The Harvard Law Review published a review in 1895 entitled, "A review of the Law of Safe-Deposit Companies." This review includes an assessment of safe deposit box safeguards. As the review stated, "The system of safeguards with which safe-deposit vaults are provided is now very complete. The mode of construction is such as to offer a very slight opportunity for entry from without by thieves."[18] The keyword in this second sentence is "without." The review is noticeably silent about the threat from within or the responsibility to safeguard an asset beyond keeping it under lock and key, or as the review terms it, "the care a 'prudent and intelligent' man would exercise in regard to his own property under similar circumstances."[18]

Figure 4. Old safe deposit boxes[17]

The review cites an 1878 decision from the Supreme Court of Pennsylvania, *Safe Deposit Company of Pittsburgh v. Pollock* (85 Pa. 391), which established the requirement in Pennsylvania for a safe deposit company to safeguard assets to prevent the "want of ordinary care."[19] The safe deposit box renter, Pollock, entered into an agreement with the Safe Deposit Company of Pittsburgh, which agreed to, among other duties, keep, " 'a constant and adequate guard and watch over and upon the safe,'" as well as, "to protect his safe, and its contents from any dishonest of the company's employees."[19] However, Pollock's box was burglarized.

During business hours and normal business operations, Pollock would be able to access his locked safe deposit box in the unlocked vault through the use of a key he alone held. After business hours, however, access to the safe would require two keys: one key held by the company to open the vault and the safe deposit box key held by Pollock. In either event, the fact that the company could not safeguard Pollock's safe deposit box led the court to determine that the Safe Deposit Company of Pittsburgh created the want of ordinary care.[19] The decision does not specifically suggest that employees participated in the burglary of Pollock's box, but it does leave open the possibility that employees acted carelessly to the extent that it led to the burglary of Pollock's box by allowing the box contents to be, "abstracted by some one entering the vault, and opening the safe by means of a key."[19]

Prior to the Harvard Law Review's 1895 mention of this case, the Banking Law Journal mentioned the *Pollock* case in 1889 in response to a question about safe deposit box liabilities for a company. The response specifically elaborated on the term "ordinary care," mentioning, among other physical safeguards, that "It is to be supposed that the rule requiring 'ordinary care' in the present instance would impose upon the bank the duty of … keeping an adequate watch over the boxes, and the exercise of prudence in the selection and employment of clerks or honesty and integrity."[20]

The *Pollock* case established case law only in Pennsylvania, yet the ruling reverberated across the country and had implications in the financial industry in the late nineteenth century. Two scholarly publications

espoused the ruling by not challenging the safe deposit box companies' contractual agreements to maintain an honest and reliable staff in a manner that a "'prudent and intelligent' man" could trust as much as him or herself. This element is covered more in-depth later as part of a discussion regarding modern practices of two-person control.

3.2 Safeguard Design

The implementation of two-person control emerged at least as early as the mid-nineteenth century, long before the Cold War or the existence of weapons of mass destruction, as evidenced by the facts surrounding the incident known as the Great Gold Robbery of 1855. In this incident, three firms, Abell & Co., Spielmann, and Butt, had gold coins valued at £12,000 in 1855, just short of £1.2 million in 2016 value,[21] stored in two safes en route from London to Paris, transported by train and ship owned by the South-Eastern Railway Company.[22]

Prior to departure from London, railroad crews weighed each firms' bullion stored in the safes. The safes travelled by train eastward from London to the British port of Folkestone. From Folkestone, a crew placed the safes on a ship that transported the safes to the French port of Boulogne. After Boulogne, the Parisian bank receiving the gold would handle its transportation.[22-24]

The safes themselves were fairly well-guarded. The two safes contained two locks. Each lock required a different key to manipulate the lock. The most contemporary account of the incident this literature review discovered, from 1859, states that the South-Eastern Railway Company provided a set of both keys to three people: a company agent in London, a company agent in Folkestone, and the ship captain transporting the safes from Folkestone to Boulogne.[23] The South-Eastern Railway Company kept keys to the safes in London and the other key in Folkestone, preventing someone from unlocking the safe while on the train.[22-24]

The three boxes of gold bullion were weighed then sealed in "heavy wooden boxes bound with iron hoops."[24] After securing the boxes in the safes, the South-Eastern Railway Company transported the safes onward to Paris. Upon arrival to Boulogne, bank officials weighed the boxes to confirm the shipment. However, officials discovered that the firms' bullion weights varied from initially reported weights in London, with one firm's box of bullion weighing about forty pounds less than initially reported and the other two weighing slightly more.[23; 24]

Railroad crews contacted the police and law enforcement began an investigation. The results of the investigation concluded that the gold was removed from the safe at some point between London and Folkestone.[22-24]

Nobody was caught stealing the gold. Sixteen months later, a career criminal named Edward Ager confessed to the crime as revenge against a co-conspirator. Ager confessed that he developed contacts within the South-Eastern Railway Company to assist him with this robbery, most notably William Tester and James Burgess (Figure 5). Ager explained his meticulously-detailed plan and how he came about obtaining both keys to unlock the safes. Ager said that Tester provided him with a wax impression of the key in London while he clandestinely made a wax impression of the second key in Folkestone that a railroad employee kept in an unlocked cupboard. Through Burgess' and Tester's involvement in the conspiracy, Ager was able to successfully defeat the safe's countermeasures and steal the gold unchallenged.[22-24]

Using the Great Gold Robbery of 1855 as a case in point, we can compare it to the three elements of two-person control. With regard to the threat to an asset, the South-Eastern Railway Company regularly

transported money and gold, subject to theft. Without such a threat, the company would not go to the lengths it did to safeguard these items. With regard to safeguarding an asset, the company took deliberate measures to implement both engineered and human safeguards through the use of safes with multiple locks and via entrusting keys to specific people. Finally, with regard to preventing human compromise, the South-Eastern Railway Company separated the keys during the train's initial journey, with one key staying in London and the other key at the destination point of Folkestone, for the purpose of preventing access during rail transport.

Figure 5. Great Gold Robbery conspirators – From left to right: William Tester, James Burgess and Edward Ager[25]

The Great Gold Robbery of 1855 provides some historical insight into the nature of two-person control as a safeguard that has been in place since at least the mid-nineteenth century. No reviews, contemporary or modern, indicate that the safes themselves were in any way unique or revolutionary, further indicating that such safes had been in use prior to 1855. It may be telling to note that even this early forerunner to modern technical systems for two-person control suffered defeat not from a failure of the engineered devices, but rather from deficiencies in administrative implementations that allowed insiders to operate undetected.

The insider threat, wherein a trusted agent uses insider knowledge or access to undermine or circumvent access control, significantly contributed to Ager's success. Tester and Burgess provided Ager with insider knowledge that Ager specifically used to steal the gold on the train. One must consider how to prevent this type of unauthorized access, even with safeguard implementations to protect an asset with an identified threat. Reviewing nineteenth and turn-of-the-century journals and case law for evidence of two-person control demonstrated, however, that one industry in particular made headway into preventing human compromise.

3.3 Preventing Human Compromise

Preventing human compromise originated from suggested regulatory procedures to minimize an organization's liability of an asset under its care and control. While one now might take for granted that preventing human compromise is an organization's responsibility with regard to safeguarding an asset safeguarded by two-person control, the practice first had to originate at some point. The oldest, most foundational document discovered intended to prevent unauthorized access within a two-person control setting was found in a presentation made in the Grand Ball Room of the Waldorf-Astoria in New York City on September 13, 1904.

A special committee formed by, and to report to, the Executive Committee of the Trust Company Section of the American Bankers' Association submitted its report regarding laws and legal decisions that surround safe deposit box companies at the Eighth Annual Meeting of the Trust Company Section in New York City in September 1904. This report notes the "scarcity of both statutes and legal decisions directly

on the subject" of "safeguarding valuable property."[26] The report continues by offering legal opinions regarding a company's duty and liability to the safe box holder, box holder rights, the manner by which liens should be interpreted, along with several other industry-specific issues.[26]

The most formulating thoughts found in this report with regard to preventing human compromise are in a section regarding a safe deposit box company's liability to box holders. Opining on a hypothetical scenario in which a safe deposit box renter claims his or her box was burgled and the renting company claims that the only person who opened the box was the renter, the report states, "Proof of this assertion by the testimony of all the company's employees who have access to the vault in which the box is kept, raises an issue as to whether the lost property, if ever in the box, was actually taken out of it by anyone except the boxholder, and this the jury must decide."[26]

To this point, the report presents the following question: "Must the boxholder, besides proving loss, prove that negligence on the part of the company occasioned such loss, or must the company, when the loss has once been proved, take the burden of showing that it is free from negligence, and even be compelled to go so far as to explain the loss?"[26] The report qualifies this question by discussing that the few court decisions that exist regarding this issue establish that, "the burden of proof is first on the boxholder (the plaintiff) to prove his loss, then its shifts to the company (the defendant), which, on showing itself free from negligence, must be relieved of liability…"[26] The report makes the point that the committee does not think that the renter should have to prove a company's negligence and the company should not have to explain the loss.

The above two statements bring to light the thought process of the committee. To the committee, the underlying concern of safe deposit box rental is not one of asset protection for protection's sake, but rather one of liability. The report sums up its thought regarding this topic with the following two sentences: "However the law may develop, the importance of taking every practical means of protecting a company from such claims is very clear, and yet how often we find attendants taking out and replacing boxes, handling both keys, the boxholder at times not even within sight. This extreme courtesy on the part of the attendants or laziness on the part of the customers, should not be encouraged."[26] Clearly, the report acknowledges that a company needs to not extend such "courtesy" to its customers as to create a situation that could bring into question an asset's loss or a company's negligence.

The issue of liability alone compelled the committee to suggest methods by which a safe deposit box can prevent unauthorized access to a safe deposit box. The report ends with a section on suggestions to stay aligned with the legal opinions offered by the special committee. The suggestions' language reflects the methods that financial stakeholders determined would best serve the legal and fiduciary responsibilities of companies employed to protect private property. Several of the suggestions deal directly with preventing human compromise:

> Never retain a key to a safe deposit box after rental.[26]

This first suggestion embodies the attempt to prevent human compromise by not allowing a person within an organization the ability to unilaterally access a safe deposit box.

> Vault, when open, should never be left without an attendant.[26]

This second suggestion again embodies the attempt to prevent human compromise by requiring that a renter is not alone in an open vault when retrieving his or her rented box, and that the company is taking care to ensure that a renter is not alone when around other safe deposit boxes.

> Vault should be opened and closed in presence of two persons, and where time-locks are used the hour should be confined by one other besides the person who attends to the winding.[26]

This third suggestion idealizes preventing human compromise by ensuring that a vault is properly sealed through the presence of one person setting the time-lock's unlock time and a second person winding the vault closed. A time-lock prevents a lock from opening, even with a correct combination, until a pre-set time of day is reached on an attached timer.

> Safe deposit boxes should always be replaced in the presence of the renter.[26]

The fourth suggestion demonstrates an organization's ability to prevent unauthorized access by allowing the renter to ensure the box is secured and inaccessible to other parties. Further, the suggestion is meant to ensure that a renter's property is determined by the renter to not have been tampered with outside of his or her presence.

This document from 1904 is the oldest foundational document found during the course of this literature review suggesting the need to prevent unauthorized access in an industry. Following this special committee's report, practices and methods of safe deposit boxes changed to adopt a view of a company's liability regarding an asset.

By 1914, the safe deposit box industry used two-person control as an industry best practice and actively prevented unauthorized access. The case in point for this is found in the facts surrounding *National Safe Deposit Company v. Stead, Attorney General of the State of Illinois*. This case involved a safe deposit box renter's death and the State of Illinois. Upon a renter's death, the State of Illinois sought inheritance taxes from the renter through assets from the renter's box.[27]

Figure 6. Modern safe deposit boxes. Safe deposit boxes became much more secure as safeguarding became more prominent. Note that each box has two locks.[28]

Arguments made in a brief by the National Safe Deposit Company to the Supreme Court of the State of Illinois included, "No renter will be permitted to enter the vaults except in the presence of the vaultkeeper."[27] Another argument made was, "the safes could be opened only by two keys, or two combinations, one of which keys or combinations was held by or known only to the renter, the other being held or known by the company's agents. So that it required the joint act of the customer and the

Company to secure access to the contents, -- the Company having no right or means of access to the box itself, nor did it possess any knowledge or information as to the ownership of the securities deposited therein."[27]

The company expressly stated that they made a practice of preventing human compromise, in that they not only had the means to do so through the requirement of two keys or two combinations for access, but they also did this as a regular practice. The company did not file a brief with the court alleging that this method of operation was out of the ordinary or otherwise unusual, indicating that it was a standard practice worthy of mention in a brief to aid their legal arguments to the Supreme Court of the State of Illinois and, on appeal, to the Supreme Court of the United States.

Although the National Safe Deposit Company lost its suit in both the Supreme Courts of the State of Illinois and the United States, the arguments made are indicative of the move toward preventing human compromise due to liability concerns within the safe deposit box industry, as well as making two-person control a regular practice in the industry.

However, no historical documents found indicate any specific practice to minimize human compromise by extraordinary means, as documented above in the more modern examples of the Brink's-Mat Heist and Northern Bank of Belfast robbery, in which the lives of the employees or their loved ones were threatened. The historical context of two-person control for asset protection with regard to human behavior appears to focus on personality traits and lifestyle factors. As will be demonstrated, this trend of reviewing one's personality traits and lifestyle factors as indicators of an employee's susceptibility to coercion continued into modern industry.

Employees hired for asset protection utilizing two-person control have the following terms associated with them in historical documentation: honesty, integrity, prudent, and intelligent. These terms tend to promote the idea of an upstanding citizen, willing to 'do the right thing' upon detecting wrongdoing. These historical documents do not associate two-person control practitioners with terms such as "lacking susceptibility to coercion" or "lacking exploitable emotional or familial bonds," which demonstrates a gap between the ideal employee and the security risks the ideal employee brings to an organization.

Each element of two-person control has been reviewed above. First, the early documented signs of a threat to an asset and an employee's need to be reliable and honest. Second, the implementation of two-person control through the Great Gold Robbery of 1855. Third, the development of preventing human compromise. With these cases all occurring from as late as the early twentieth century, this literature review will now explore the modern day practice of two-person control.

4. TWO-PERSON CONTROL IN MODERN INDUSTRY

Following a brief review of its early history, the evolution of two-person control will be reviewed as practiced in several modern industries using the elements identified in Section Two. These industries range from financial to biosecurity.

4.1 Financial Industry

4.1.1 Threat to an Asset

The financial industry faces threats from outside and within. Determined criminals still rob banks. As well, bank employees still collude as insiders to steal customers' money.

Financial institutions safeguard several high-value assets beyond just cash. Banks still rent out safe deposit boxes, which hold items other than money (Figure 6). For example, a safe deposit box can hold a renter's valuable jewelry, bonds (such as was the case of Pollock, mentioned earlier), or even corporate trade secrets worth much money to competitors. While not specifically related to the financial industry, safe deposit boxes contain items well beyond the scope of financial professionals; however, the financial industry is the industry that currently provides asset safeguarding for private persons and companies with valuables to store.

The threat of bank robberies is very real. A 2015 Federal Bureau of Investigation's (FBI) Bank Crime Statistics summary notes that 2014 saw over four-thousand reported robberies, burglaries, and larcenies at banks in the United States. Robberies constituted 3,961 of these incidents. Of particular interest is that 174 of these incidents involved a bank's vault.[29]

4.1.2 Safeguard Design

The financial sector utilizes two-person control procedures for safeguarding many assets. Rather than calling the procedures "two-person control," though, the financial industry uses the term "segregation (or separation) of duties." Segregation of duties relies on the same principle safeguarding methods of two-person control: engineered or human implementations. A Federal Deposit Insurance Corporation (FDIC) document, Risk Management Manual of Examination Policies, states in a section called Internal Routine and Controls that, "A segregation of duties occurs when two or more individuals are required to complete a transaction."[30] This action, according to the document, allows one's work to be verified by another as, "properly authorized, recorded, and settled."[30]

A 2010 Ernst & Young report titled, "A risk-based approach to segregation of duties" acknowledges that "the increased interest in SoD [segregation of duties] is due, in part, to control-driven regulations worldwide and the executive-level accountability for their successful implementation."[31] Clearly as a continuation of the safe deposit companies' liability with regard to rented boxes, the financial industry identified that liability and accountability are inherently connected with their duties as safeguard providers.

Regulations the Ernst & Young report cites are the Sarbanes-Oxley Act of 2002 (SOX), a legislative act to minimize an institution's and consumers' financial risks. After Arthur Andersen conducted poor audits of Enron and WorldCom, both of which led to the largest Chapter 11 bankruptcy filings of their times, the

United States Congress passed SOX, which required, "public companies to obtain an independent audit of their internal control practices."[32-34]

The requirement of an independent audit for another company's internal control practices is very similar to that of an engineered implementation of two-person control. Internal control is defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), an enterprise risk management, internal control and fraud deterrence think tank, as, "a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance."[35] A COSO report lists one of the operational objectives of internal control as "safeguarding assets against loss" at it relates to an entity's effectiveness and efficiency. [35]

The Ernst & Young report adds, "the underlying reason for these regulations is more important: no individual should have excessive system access that enables them to execute transactions across an entire business process without checks and balances. Allowing this kind of access represents a very real risk to the business…"[31] This statement clearly reflects the meaning of establishing two-person control from a liability perspective, much like the American Bankers' Association report recommending the implementation of safeguards for the safe deposit box industry.

Financial institutions are encouraged to maintain the best practices of two-person control for regular banking operations. These operations include opening and closing a bank branch, monitoring customers with safe deposit boxes, and requiring confirmation for certain financial transactions. These practices are human implementation safeguards. In fact, these are so commonplace that a financial consulting website openly offers suggestions on how to implement opening and closing procedures, as well as methods for two employees to verify certain types of financial processes performed by each other.[36-38]

A security consultant for credit unions offers suggestions for a credit union's opening procedures: have one employee enter a branch alone in the morning, while a second employee acts as a watcher. The first employee should lock the door to the bank and check the inside to make sure everything is in order. The two employees should have each other on the line via cell phones while the first employee is inside. The watcher should wait for the first employee to exit the branch to give an all-clear sign, indicating that everything is normal. After giving this sign, the first employee should re-enter the bank and lock the door, requiring the watcher to unlock the door prior to entering.[39]

This opening procedure is done for safety and, to what is important here, security reasons. Should someone enter the bank while the first person is in the bank alone, the watcher can observe this and immediately call the police. Additionally, should the person enter the bank and try to coerce the first employee, still alone, to open the vault, the employee would not be able to open it since the watcher is not present. If the first employee doesn't return within a pre-designated set amount of time, the watcher can immediately call the police.

4.1.3 Preventing Human Compromise

While the financial industry had an interest in preventing the hiring of "dishonest" employees as far back as the late-1800s, one's honesty today is not very transparent. Financial institutions still to this day seek employees not in financial or criminal straits to ensure a bank's financial assets are secured by a trustworthy agent.[40; 41] While two-person control appears to be a best financial practice, the Ernst & Young report cited above admits, "a company cannot eliminate every potential risk."[31] Financial institutions have an interest in ensuring their employees are not in dire financial straits or have unfavorable criminal histories.

However, the government relations director for TransUnion testified to Oregon legislators in 2010 that, "'At this point, we don't have any research to show any statistical correlation between what's in somebody's credit report and their job performance or their likelihood to commit fraud.'"[41] A case in point for this statement is that, even after vetting an employee to determine his or her trustworthiness, bank robberies still occur and bank employees still conspire with fellow employees to embezzle money.[42-44] Incidents like these occur even as the financial industry is among the most highly regulated industries in America.[45]

4.2 Information Technology Industry

4.2.1 Threat to an Asset

Information technology (IT) assets are numerous and face critical threats. The IT industry integrates in some way with almost everything we do on a daily basis, and this integration increases daily. Critical communications and infrastructure are tried to the IT industry as are critical databases, such as an organization's human resources database.

Consider Terry Childs, the sole critical network administrator for the City and County of San Francisco, who, in 2008, singlehandedly shut out the entire City and County from its computer networks, including citywide payroll information and police records, for weeks. Childs was the only person in possession of network keys. Even after his arrest and jailing, Childs initially refused to provide the network access keys, eventually providing them directly to then-Mayor Gavin Newsom.[46; 47]

Critically, supervisory controls and data acquisition, or SCADA, systems are controlled by IT infrastructure. A type of industrial control system, SCADA systems control automated industrial processes, such as an oil pipeline's flow volume, or an electric power grid's ability to distribute electricity between points. These SCADA systems have become more popular, but still face threats. For example, a computer virus physically destroyed centrifuges in Iran that were running on SCADA systems. As well, three independent electric grids operated by SCADA systems span the continental United States: the Western, Eastern, and Texas Interconnections.[48; 49]

A survey of SCADA systems conducted by the SANS Institute found that seventy percent of respondents consider the risks to their SCADA systems as "high to severe" and that one-third of them suspected "they may have had incidents."[50] Forty-one percent of the 198 incidents reported to the United States Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), a Department of Homeland Security entity, targeted the energy sector, and twenty-three of these energy sector attacks targeted industrial control systems.[50]

In addition to physical systems controlled by cyber means, cyber systems themselves face threats. For example, denial of service attacks, viruses, and ransomware can maliciously affect virtually any digital network. One system implementing multi-person control, domain name system (DNS), allows internet users to safely and securely browse websites using a text-based name as opposed to an internet protocol (IP) address by translating a text-based name into an IP address that a computer can use to connect to a specific network or website[**] and will be covered in the next section. Safeguarding DNS is DNS Security (DNSSec), which uses digital cryptographic keys to ensure an organization implementing DNSSec works to prevent malicious actors exposing networks to cybersecurity threats.[51; 52]

[**] A simple analogy to describe DNS functions would be using a phone book to look up somebody's phone number: a phone book contains Matthew's name and his associated phone number. Mark can connect with Matthew using the phone number associated with Matthew as provided in the phone book. This phone book-type of association is also known as 'address resolution.'

The risks and consequences associated with information technology infrastructure are very significant in modern American society. The basic ability of first responders to assist in an emergency situation could be crippled in an instant, and automated controls running critical infrastructure could simply shut down.

4.2.3 Safeguard Design

Two-person control in the information technology (IT) industry is widely referred to as separation of duties, just as the financial industry refers to two-person control as segregation of duties. As opposed to the financial sector in protecting assets such as currency or other valuables physically stored in safes, the role of two-person control in the IT industry acts as a check and balance to unilateral overall system control.

Role-based access control (RBAC) is an important feature in the field of system administration, and is described as "the evolution in the field of access control." It is "considered a natural mechanism for the implementation of separation of duty."[53] As a researcher writes, "According to the concept of separation of duty, a business process or task is divided into more than one sub process or sub task. These sub tasks are assigned to different roles and different users are assigned to these roles. These roles are declared mutually exclusive to each other, i.e., these roles will not be active by a single user at the same time."[53]

Industry professionals have explored the two-person control concept in the IT industry since at least 1987 with research performed by Clark and Wilson.[54] Several studies, such as Role-Based Security, Object Oriented Databases & Separation of Duty,[55] Separation of duties for access control enforcement in workflow environments,[56] Access Control: Principles and Practice,[57] and Two-Person Control Administration: Preventing Administration Faults through Duplication,[58] among a host of others, discuss the separation of duty concept in the database administration setting.

Potter, Bellovin and Nieh's study on a particular RBAC system did stand out. This study tested a system in which every administrative change made to a system by administrator A had to be similarly made by administrator B in order for the change to be introduced into the system. The authors call the system "ISE-T (I See Everything Twice), a system that applies the two-person control model to system administration."[58] Such a system, per the authors, will reduce the likelihood of faults or errors in system-wide changes. As well, the system will reduce the ability of malicious actors from sabotaging systems or establishing a back door for one to gain higher user privileges than granted at that time. However, this system by itself and without other elements of two-person control would not protect the system from colluding administrators.

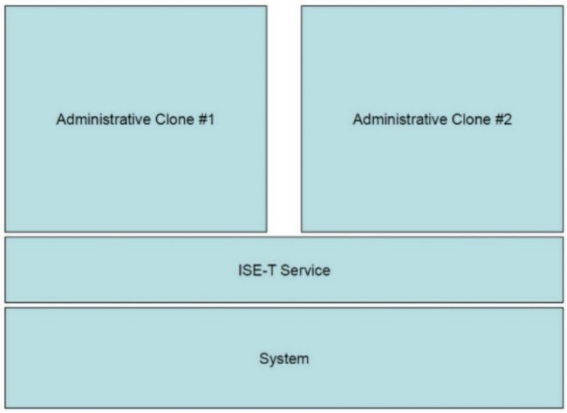

Figure 7. Potter, Bellovin and Nieh's ISE-T system[58]

The driving force behind the ISE-T concept is that the system is cloned, allowing an administrator to review the same environment, so to speak, rather than a duplicated system that is independent of the original (Figure 7). Two administrators must make the same change to a system in order to validate the change and implement it. For example, elevating a non-administrator's user privilege would require two administrators to take the same action, that is, take the same steps to change that user's privilege settings. This is opposed to a system in which an administrator makes a change and another administrator simply approves the change.[58]

Not only do the authors argue that this ISE-T system will reduce errors and faults in system administration, but will help with training new system administrators by requiring they take the appropriate steps in order for action validation.[58]

Should one administrator's change not match up with another's, a system reboot will delete the modified and non-validated change. These actions range from software installations, and system configurations to malicious system exploits. The researchers set up their desired system and asked users to create a back door into the system without specifying anything about the type of back door used. As the users all created different types of back doors and placed them in different system locations, the ISE-T system detected all changes from all users, since no users duplicated one another. Had this been a company's system, the ISE-T system would have prevented several malicious actors from installing a host of back door access points into the company's entire computer system.[58]

Safeguard design within the IT industry did not limit itself to RBAC processes. In 1979, Adi Shamir proposed a method for splitting a secret into n shares, any $k \leq n$ of which can recover the original secret, but any $k-1$ or fewer shares, when combined, will have no knowledge of the secret. In other words, if a secret is split into twenty shares and a minimum of eight shares are required for recovering the secret, seven shares will not allow for one to recover the secret; only eight or more shares will allow for the secret's recovery. The paper also discusses threshold schemes associated with reconstructing this divided data, such as tradeoffs in cryptographic key management between the balance of "secrecy and reliability," and "safety and convenience of use."[59] The benefit of such a concept allows for dividing an asset's safeguard between several different points, requiring one to possess a pre-determined number of shares to access an asset.

One great example of this is found in how address resolution[††] is safeguarded. Disabling DNSSec would essentially shut down the global ability to browse the internet. The Internet Corporation for Assigned

[††] To continue with the phone book analogy: after Matthew dials the phone number associated with Mark as found in the phone book, Matthew's phone line goes through a process to connect with Mark's phone line that allows

Names and Numbers (ICANN) safeguards DNS by encrypting a DNS recovery key using secret sharing. On top of physical safeguards that include locking smartcard keys in safes inside a secure room guarded by biometric, keycard, and knowledge-based access controls, ICANN provides recovery key shareholders, "trusted community representatives,"[60] with smartcards that each contain a share of the DNS recovery key. Out of at least twenty-one trusted community representatives, ICANN requires a minimum of five recovery key shareholders to access the recovery key. No fewer than five shares will allow for worldwide DNS recovery should DNSSec on root DNS servers unexpectedly fail.[51; 60-62]

A more recent publication on secret sharing proposes a method, titled, Serial Interpolation Filter, that expands on secret sharing concepts mentioned above, while allowing one to "operate over set-oriented data distributed across multiple repositories without exposing the original data."[63] In other words, the paper demonstrates a method of allowing one to access an item using secret sharing without requiring the original item to exist at all in any one place prior to sharing. Further, the method ensures data security resulting from "various attacker models,"[63] including collusion. Digital information is broken up and stored, in parts, on multiple servers, and can throw off colluding insiders. For example, a key holder could inquire with the minimum number of shareholders to confirm information from their shares that allows the key holder to access an item, such as a list of names, without any shareholder possessing the ability to recover the list. Shareholders, in turn, have no way to determine the minimum number of shares required to recover the original secret.

4.2.4 Preventing Human Compromise

With regard to preventing human compromise,

As mentioned above with regard to ICANN entrusting twenty-one trusted community representatives, the ability to recover the internet from a massive cyberattack rests with a small group of people with experience in DNS security who have a stake in the continued success of DNS. For example, trusted community representatives in 2010 included thirty-four IT stakeholders (twenty-one primary stakeholders with thirteen back-ups) from, intentionally, all around the globe.[51; 60-62]

This literature review did not discover any specific or noteworthy practices within the IT industry regarding employee vetting or reliability. However, certifications, such as Certified Information Security Auditor (CISA), Certified Information Security Manager (CISM), and Certified Information Systems Security Professional (CISSP), are a steadily increasing requirement for many IT system administrator positions. An employer can rely on the dependability of the issuing organization to ensure that the certificate holder can perform the certified IT functions, "a logical way to verify your [a job seeker's] skills and knowledge."[64]

Certifications alone do not ensure that an employee will protect his or her access to an asset properly, though. In the Childs case mentioned above, Childs possessed a Cisco Certified Internetwork Expert certification, but was either not subjected to a rigorous vetting process, or those hiring him determined what was known about his behavior and criminal history did not overly concern them. For example, Childs was arrested and convicted for aggravated burglary, spending four years in a Kansas state prison. Childs was arrested again in 1995 for aggravated assault and weapons charges. Additionally, Childs had an altercation with the IT department's security manager, Jeana Pieralde, in the weeks before he locked the City and County out of its networks. At one point, Pieralde feared for her safety and locked herself in one of the building's rooms and called for help. Childs denied the events as Pieralde described them and claimed Pieralde was snooping in peoples' workspaces.[46]

Matthew and Mark to speak with one another. This process is akin to address resolution.

4.3 Civil Aviation Industry

4.3.1 Threat to an Asset

Within the context of two-person control, civil aviation faces the threat of hijacking or other form of intentional crashing.

Per the National Commission on Terrorist Attacks Upon the United States, popularly known as the 9/11 Commission, "In the year before 9/11 the FAA [Federal Aviation Administration] perceived sabotage as a greater threat to aviation than hijacking. The Commission found that a 1996 presidential commission on aviation safety and security chaired by Vice President Al Gore "reinforced the prevailing concern about sabotage and explosives on aircraft."[65] In hindsight, this seems to be a very frustrating lack of the obvious, but consider the frame of mind at the time: no hijackings had occurred domestically in over a decade and international hijackers tended to land planes to make demands for hostages; the hijackers did not kill themselves or tend to kill hostages. This made explosives appear as a deadlier threat than hijackings.[65]

Prior to September 11, 2001, however, civil aviation still faced the threat of suicide pilots. One major airplane crash on October 31, 1999, killed over two-hundred people. The crash of EgyptAir Flight 990 revealed that a recently-reprimanded pilot, Gamil el-Batouty, who was not in the cockpit for the first portion of the flight, appeared to wait until a senior pilot left the cockpit. Upon the senior pilot's exit, el-Batouty entered the cockpit and ordered a younger first officer to leave. After the first officer left, el-Batouty, now alone, turned off the autopilot and put the plane into a nose dive to the ground from 24,000 feet above. A member of the National Transportation Safety Board team told the UK Guardian that el-Batouty appeared to act out of revenge, indicating that he acted very intentionally, as opposed to the airplane crashing due to mechanical failure.[66]

Along these lines, there are at least seven more documented instances of pilots killing themselves, anyone on board and anyone on the ground where the airplanes hit. One report from March 26, 2015, notes that since 1976, 416 people have died as a result of non-mechanically-related intentional crashing.[67] Not included in this report is a plane crash that occurred that very day: Germanwings Flight 4U9525's crash into the French Alps.

Figure 8. Chart of intended route for Germanwings Flight 4U9525[68]

A Germanwings co-pilot, Andreas Lubitz, crashed the AirBus 320 he piloted into the French Alps while flying from Barcelona to Dusseldorf (Figure 8). Lubitz was alone in the cockpit after the pilot needed to use the restroom, allowing Lubitz to turn off the auto-pilot function and begin a descent from 38,000 feet to 100 feet.[69] Lubitz denied the pilot access back into the cockpit by overriding the pilot's emergency code on the cockpit door to re-enter after Lubitz refused him re-entry. This override function put the cockpit door into a lockdown mode, which could not be overridden by those outside for five minutes once activated and left Lubitz alone for the remainder of the flight.[70; 71]

4.3.2 Safeguard Design

Two-person control for airplanes with two pilot seats, now mandated in the United States by the Federal Aviation Administration (FAA), is a best airline practice in the United States. This system manifests by having at least two people in the cockpit on airplanes with two sets of pilot controls. Unfortunately, the aviation industry has several instances of a rogue or lone pilot taking his or her life, along with anyone else who happens to be on the airplane at the time, so the need to watch over a pilot became critical.

At the time of the incident, American, Canadian and European regulations did not require airlines to have more than one pilot in an airplane's cockpit. The Air Line Pilots Association, which represents pilots of United States carriers, said that each airline in the United States ensures that more than one person remains in the cockpit of an airplane designed for two pilots. The practice was optional at the time in Canada and across Europe, as well, and up to individual carriers to make the choice for a two-person in the cockpit rule or not. All American carriers implemented the practice, but not all Canadian or European carriers did.[69; 72]

Though not required in America by the FAA at the time, the FAA spelled out its stance in an administrative document regulating certificate authorizations one must possess to enter a cockpit. The document, dated January 28, 2015, details that a certificate authorizing entry into a cockpit must, in part, state the procedure "for two person flightcrews, when one flightcrew member leaves the flight deck."[73] This policy demonstrates that the practice was a known and standard practice in the industry, but the policy did not require its implementation, as noted by the passive language simply requiring a certificate to outline procedures to follow. These procedures would derive from individual carriers, which have the option to enforce a two-person rule.

Just days after the Germanwings incident, however, Transport Canada, Canada's regulatory body for aviation, ordered all airlines to maintain a two-person rule for the cockpit.[69] Within a few days of Canada's adoption of a requirement to enforce a two-person rule for the cockpit, the Federal Aviation Administration revised its administrative document noted above to now require two people in the cockpit at all times, as noted by the revised language that a certificate authorizing entry into a cockpit must state the procedure "to ensure two persons are always on the flight deck. For two-person flightcrews, this means when one flightcrew member leaves the flight deck, another individual that is qualified… must be present to lock the door and remain on the flight deck until the flightcrew member returns to his or her station."[74] The language used requires the use of the two-person rule in the cockpit and does not give an American airline the option to not put it to use.

The European regulatory agency for aviation, European Aviation Safety Agency (EASA), did not require to have more than one pilot in an airplane's cockpit, but as with American and Canadian carriers, individual airlines do. Unlike American carriers, however, only a handful of airlines enforced such requirements. Lufthansa, Germanwings' parent company, did not have this requirement. Short of requiring airlines to adopt two-person control for pilots, European regulators have strongly recommended that airlines re-visit individual corporate policies in light of the Germanwings incident. Regulators in the

United Kingdom, slightly more emphatic than the EASA, urged airlines to adopt a two-person rule for the cockpit, but the U.K. Civil Aviation Authority cannot enforce these urges or suggestions.(75)

4.3.3 Preventing Human Compromise

The European Cockpit Association, which represents 38,000 European pilots in thirty-seven European nations, actively opposed EASA's two-person rule measures recommendation following the Germanwings incident, citing that such measures introduced new risks into existing security measures, such as the introduction of a flight crew member with no knowledge of how to operate an airplane or not necessarily subject to as stringent of a background check as pilots.(76) This concern illustrates the concern that a lone crew member who has not undergone a stringent background check, knowing that he or she will have access to the cockpit at some point when a pilot steps out, could act maliciously once he or she accesses the cockpit due to coercion or deliberate intent.

Following this European Cockpit Association policy position from February 2016, the EASA released results of a stakeholder survey regarding a two-person rule for airplane cockpits. The vast majority of survey respondents, eighty-six percent, identified as pilots. The survey results found that European airlines did, for the most part, implement a two-person rule for cockpit safety following the EASA recommendation to do so. However, pilots by and large rejected the effectiveness of a two-person rule for reasons of introducing new security threats or for specific reason. The survey's last question asked why a two-person rule should not become mandatory, to which a significant number of pilots responded that the rule "introduces more risks than it mitigates."(77) Without specifying in detail, some of these risks presumably include allowing an untrained pilot to gain access to the flight deck, thereby creating a risk to the plane either through malicious intent or accidently manipulating buttons on the flight deck.

Faced with a backlash of stakeholder opinion, the EASA proposed in late 2016 that individual airlines determine the need to regulate their own need for two people in the cockpit at all times following the psychological screening of their own pilots.(78) An EASA opinion, which is not legally binding, proposed in December 2016, that air crews conduct "preventative measures" that include "carrying out a psychological assessment of the flight crew before commencing line flying."(79)

Human reliability, through the lens of mental health, became a major topic in the civil aviation industry following the Germanwings incident. The international aviation industry is currently undertaking a review of steps by which carriers determine what qualifies a pilot as reliable and the built-in safeguards to implement as a best practice. Airlines in the United States and Canada have a standard of two-person control as a best practice that European regulators do not implement. Two-person control as a whole, and not just mitigating the element of a threat through mental health screenings, is becoming the industry standard and a best practice in the civil aviation industry. Taking one action, mitigating the threat, but not implementing or regulating the two-person rule for cockpits, leaves a gap in safeguarding the airplane. For example, Lubitz, the Germanwings pilot who crashed the plane, was found to be "100 percent fit" for duty per Lufthansa's records.(72)

As mentioned previously in this review, an employee's reliability is very important in enforcing two-person control. As far back as the nineteenth century, companies using early methods of two-person control implemented policies describing the need for honest employees. The term "honesty" as used in the *Pollock* case to demonstrate the required character for an employee expanded over the years to require inquiries into more than just one's sense of morality and ability to tell the truth. Many organizations now wish to know more about an employee's personal history and reliability through demonstration of one's work history, criminal history, financial affairs, social interactions and mental stability. Such measures work as a safeguard against hiring a dishonest or easily coercible employee. While many companies and organizations conduct basic background checks for employment and criminal history, the remaining

industries reviewed implement more extensive programs to determine an employee's reliability as described above in this paragraph.

Figure 9. Cockpit Door Keypad[80]

Cockpit doors have increased in durability and accessibility since September 11, 2001, when hijackers forced their way into four airplane cockpits. Cockpits require one to enter a code for access, which flight crew members have in case a pilot becoming incapacitated (Figure 9). In the case of a security-related emergency, such as if hijackers demanded entry into the cockpit and attempted to coerce a flight crew member to enter his or her code, a pilot can prevent anyone from entering a code using an override function that will disable the keypad for up to five minutes.[81]

As seen in the Germanwings crash, though, the cockpit's occupant, one bent on suicide for himself and the entire plane, successfully locked out an authorized pilot for five minutes using this override function. Five minutes was more than enough time for Lubitz to crash the plane.

4.4 Gaming Industry

4.4.1 Threat to an Asset

Considering the threat to a gaming industry's asset, one might envision an *Ocean's Eleven* scenario, in which a nondescript group of criminals use an incredibly intricate ruse to gain access to a casino's vault, only to casually walk away from the casino millions of dollars richer. Threats facing the gaming industry are similar to the threats posed in the fictitious *Ocean's Eleven*-type scenario, in that casino vaults are burgled and robbed, though these burglaries and robberies tend to not be performed with nearly as much flash and pizazz as a Hollywood rendition would have one believe. Threats against casinos tend to be ones involving violence or the threat of violence, classifying the crimes as robberies.

Additionally, the gaming industry has several documented cases, two of which will be briefly reviewed, indicating that the insider threat looms large within the industry.

4.4.2 Safeguard Design

As casinos store large sums of money in vaults, casinos implement two-person control through engineered and human-based methods. Matthew Bunn and Kathryn Glynn's 2013 published study on the insider threat describes best practices in the gaming industry as implemented by casino security managers.[82]

Engineered implementations include heavy vault doors, impeccable surveillance methods, and access control throughout the casino's back rooms.

Human implementations include the use of dual concurrence, in which two people from different organizations within the casino must agree to perform the same action or conclude with the same result. Examples of required dual concurrences include entering or leaving a vault, cash and chip transfers, and signatures agreeing to the count of cash or chips. Another built-in safeguard includes the use of a two-person system that requires people from unrelated organizations within the casino to observe the count of money. Oftentimes, this includes a cashier and a member of the state's Gaming Commission.[82]

Safeguards designs in gaming establishments do vary in stringency and not all casinos appear to implement similar levels of safeguard designs. To demonstrate this point, one can consider the facts surrounding three successful casino robberies between the years 1997 and 2007 affecting the gaming industry: the 1997 robbery of the Caesars Palace Hotel-Casino in Las Vegas, Nevada; the 2004 robbery of the Taj Mahal Casino Resort in Atlantic City, New Jersey; and the 2007 robbery of the Soboda Casino in Riverside County, California.

The facts surrounding the 1997 robbery of the Caesars Palace Hotel-Casino in Las Vegas, Nevada, showed that high-value assets were safeguarded by use of a two-person rule, in that physical transportation of assets was subject to a two-person rule, as was access to the casino's vault.[83] The 2004 robbery of the Taj Mahal Casino Resort in Atlantic City, New Jersey, and the 2007 robbery of the Soboda Casino in Riverside County, California, demonstrated that one person can unilaterally access an area securing high-value assets.[84; 85]

In the 1997 Caesars Palace robbery, a masked man with a gun successfully robbed two casino security guards transporting money between casino cages.[83]

The 2004 Taj Mahal robbery involved an insider who stole an employee access card and gave it to the eventual robber, along with the date and time when the casino's deposit bag would be in the general cashiering office. This robber used the card to access the general cashiering office at the given date and time to gain access to this secure area of the casino and steal the bag full of money. The robber defeated an engineered safeguard by gaining unauthorized access to a restricted area.[84]

The 2007 Soboda Casino robbery was committed by an insider, as well. A low-level security technician with financial problems forced his way into the casino's vault with a gun and physically restrained four employees. The employee left the casino with over $1 million.[85]

4.4.3 Preventing Human Compromise

According Bunn and Glynn's study, a majority of employing organizations screen employees through background checks. These checks range from criminal history checks to full background investigations that include financial, social and mental health checks. In many casinos, employees undergo reinvestigations every few years in order to maintain their ability to work in their casino.[82]

Casinos have an interest in knowing an employee's financial troubles and with whom an employee associates, in that a casino will likely not place an employee with financial burdens or associates with fraudsters in a position that would put the employee in proximity to money.

Even with extended background checks, though, employees still cannot be completely trusted. Two robberies referenced above were successful largely due to the active or complicit insider. As the representative of the Luiseno Indians said with regard to the Soboda Casino robbery, "'The suspect was cleared to work here by many security measures, but sometimes decent people do bad things.'"[85]

4.5 Pharmaceutical Industry

4.5.1 Threat to an Asset

Bunn and Glynn's study also reviewed the pharmaceutical industry, specifically measures taken to protect the active pharmaceutical ingredient (API) in manufacturing facilities. The API is regulated material and categorized as a Schedule II controlled substance. In the U.S., the Drug Enforcement Agency (DEA) is the primary regulator of many API and maintains influence on a manufacturer to safeguard API.[82] The DEA describes Schedule II controlled substances as ones with "a high potential for abuse which may lead to severe psychological or physical dependence," and includes such substances as morphine, methadone, opium, amphetamine and methamphetamine.[86]

The lack of continual follow-up of an employee's background appears to present a threat to safeguarding API due to a "halo effect"[82] among manufacturing employees, which will be discussed shortly. This creates an insider threat that not only costs an API manufacturer money, but stolen API in general contribute to an American epidemic of drug-related overdoses that in 2010 finally surpassed the number of "deaths attributed to motor vehicle accidents, homicides and suicides."[87] Specific to API, overdose deaths from opioids, such as methadone, "were involved in about 3 of every 4 pharmaceutical overdose deaths (16,651), confirming the predominant role opioid analgesics play in drug overdose deaths."[88]

Contracted drivers not employed by manufacturers transport API prescription medications to customer-facing pharmacies (Figure 10). Several recent reports note that pharmaceutical delivery vehicles are experiencing a rising number of thefts and robberies.[89; 90] As one report notes, "Hitting the right pharmaceutical courier can yield a payoff similar to robbing an armored car."[91] The report notes that drivers of delivery vehicles have minimal security and do not work within a two-person control framework, so the method of asset transportation does not use safeguards through engineered or human implementations. The dollar amount of drugs stolen from a delivery vehicle represent a weakness in safeguarding API.

Figure 10. Still image from video showing robbery of pharmaceutical delivery driver. Courtesy of Boynton Beach Police Department, Florida[91]

4.5.2 Safeguard Design

Bunn and Glynn note similar engineered and human implementation safeguards within the pharmaceutical industry as the gaming industry. Engineered implementations include storing API in vaults requiring two authorized employees for entry and relying on surveillance camera systems to add a layer of security to help safeguard API.[82]

As previously stated, the DEA is the primary API regulator with influence on API manufacturers. This influence extends not only to regulating the substances, but to the "design and construction" of API facilities.[82] The DEA has the ability to input its engineered implementations in manufacturing facilities.

The majority of safeguard designs within the pharmaceutical industry appear to rely on human implementation. The primary human implementation used with regard to API is dual concurrence. Some examples of dual concurrence within the pharmaceutical industry include requiring two people to enter a vault containing API, counting the removed or added amount of API's weight, securing API and transporting API between different points within the manufacturing facility.[82]

Similar to methods of dual concurrence used in the gaming industry, an employee must have at least one other person verify the weight of API that was added or removed from a secured room that also had to be entered with at least one other person. Transporting API between two points in the production facility requires two people, as well. Violating company policy through failure to abide by dual concurrence could lead to the employee's termination with that company and failure to work in the pharmaceutical industry in the future.[82]

One noted difference between the gaming industry and pharmaceutical industry, though, with regard to safeguard design, is the use of integrated enforcement teams and line inspections. Controlled substance teams, which include representatives from security and compliance teams, as well as law enforcement professionals, "are assigned to every pharmaceutical production site handling Schedule II substances."[82] Bunn and Glynn note that these teams play the role of auditors, "charged with ensuring that the company complies with both the letter and spirit of relevant regulations."[82]

Quality assurance provides, "an element of theft prevention" through random checks of manufactured pills, and reporting of any identified inconsistencies in a pill's chemical design.[82] Should quality assurance team members identify an irregularity in a pill's chemical consistency, they are required to contact the Food and Drug Administration (FDA) for follow-up. The FDA can conduct further site inspections, including observation of the fermentation and chemical synthesis processes to ensure accurate methods of production.[92]

4.5.3 Preventing Human Compromise

Background checks for pharmaceutical employees handling API include checks into an applicant's criminal and financial background, as well as an applicant's history of substance abuse. Additionally, the industry relies on employee certifications and professional licenses to ensure employees do not act improperly with API. The industry will blacklist employees fired for suspicious or dishonest activity regarding controlled substances, including API, so previously-fired employees at another API company will not be re-hired.

Once vetted, however, Bunn and Glynn's study suggests that the industry appears to be "falling victim to the halo effect"[82] with regard to personnel reliability. The study found that all interviewed security managers appeared to rely on an employee's desire to maintain his or her credentials and professional licenses as inherent deterrents to insider crime. As the study states, "most employees are professionally licensed pharmacists and pharmacy technicians, bound by the ethical standards of the American Pharmacists Association (APA), and keenly aware that a breach would result in the loss of their licenses."[82]

This literature review found no information regarding efforts to prevent unauthorized access to the API delivered by offsite delivery services.

4.6 Chemical Weapons

4.6.1 Threat to an Asset

Perhaps the most well-known examples as portrayed in popular media regarding two-person control exist within the military setting. The military stores items that can wreak much havoc in the world if accidents to certain assets occur or malicious actors gain access to these assets. These items include chemical weapons.

Chemical weapons are used by state and non-state actors alike. The governments of Iraq and Syria are accused of using chemical weapons on their own populations. In 1988, up to twenty Iraqi fighter planes reportedly dropped chemical weapons on an Iraqi Kurdish city's population, killing thousands.[93] Syria was recently accused of using chemical weapons against its own population.[94] The Islamic State of Iraq and the Levant (ISIL) reportedly used chemical weapons in Iraq and Syria.[95] Perhaps the most infamous non-state actor's use of chemical weapons is the Japanese religious cult Aum Shinrikyo, when cult members released sarin gas on a Tokyo subway in 1995. Aum Shinrikyo had used chemical weapons in a smaller-scale attack the previous year, as well.[96]

The military has an obligation to ensure that its weapons of war are properly safeguarded. Deadly assets are very contained and regulated, as will be demonstrated; however, threats to its assets remain. Outsiders and insiders both steal military arms and equipment. In one theft from a French military base, thieves made off with explosives, grenades, and detonators. In another case, United States soldiers and

civilian Department of Defense employees conspired to steal and sell Army equipment, including the sight for a grenade launcher.[97-99]

4.6.2 Safeguard Design

The military makes use of both engineered and human implementations for safeguarding its high-value assets.

Engineered implementations are numerous. Chemical exclusion areas require the use of at least two "reliable security access control devices" that can include a card reader system, numerical key pad, locks or biometric devices. Chemical munitions subject to the Department of Defense's two-person rule require storage in secured containers or approved storage devices within chemical exclusion areas.[100]

Additionally, chemical weapons storage restricts the two binary agents of a chemical weapon from being stored together.[101] Binary agents are the two chemical agents required to activate a chemical weapon's lethality. Preventing the two agents required to render a chemical weapon dangerous from being stored in the same location not only prevents the chemical weapon from accidentally discharging, but also increases its safeguarding by separating the dangerous precursors.

Human implementations appear to rely on requiring two people to be physically present during maintenance or transportation of an asset, doubling as both a safeguard and safety mechanism. Multiple instructions call for the creation and enforcement of areas requiring the "two-person rule," through the creation of chemical exclusion areas and areas containing chemical agent munitions.[100] For example, a 1987 report titled, "Chemical Munitions Requirements for the Marine Amphibious Force (MAF)" specifies that "two persons must be physically present and within observation range of each other to preclude unauthorized tampering with the projectile and to watch for signs of chemical agent poisoning."[101] This document requires that all peacetime movements enact a two-man rule for each vehicle carrying chemical munition, allowing operational requirements to determine asset security during movement during wartime.[101]

The report details chemical weapons' movements during peacetime as requiring "Technical escort teams consisting of formal school trained personnel."[101] Escort team responsibilities include, among other things, the need to inspect or certify cargo vehicles, which would not be the first industry reviewed in this literature review using inspection teams to maintain quality or control.

4.6.3 Preventing Human Compromise

The various branches of the military use reliability programs, as will be demonstrated throughout the rest of this section. A 2016 Department of Defense directive regarding "Security Standards for Safeguarding Chemical Agents" spells out the requirements in several places for maintaining a system of two-person control. One of the policies enforced regarding two-person control is implementing the chemical personnel reliability program. To pass this program, one must meet "Emotional and mental stability, trustworthiness, physical competence, and adequate training to perform the assigned duties."[100]

The "Chemical Munitions Requirements for the Marine Amphibious Force (MAF)" report notes that, "the chemical PRP [personnel reliability program] requirements are the same as those for the nuclear program."[101] The next section will review nuclear reliability programs.

4.7 Nuclear Weapons Industry

4.7.1 Threat to an Asset

One cannot discuss two-person control in the military without reviewing nuclear weapons procedures. The image of two military personnel sitting side-by-side awaiting an order to launch is very popular in movies and television. For this reason, it seems, more than any other, the concept of two-person control is thought to be primarily one of military use for nuclear weapons. As discussed, though, the concept and practices of two-person control were already established at least nearly a century before mankind even first split the atom.

Many threats to nuclear assets are obvious: theft, damage, and intentional activation. From the earliest days of the nuclear weapons industry, scientists and military personnel realized the threat of such a powerful device once in the hands of a lone actor. Specifically, as will be seen, the United States took action to ensure that nuclear weapons could not be controlled by any one specific person, without regard to that one person's responsibility to safeguard nuclear weapons. Tellingly, threats to nuclear assets are found in the justification for safeguard designs.

4.7.2 Safeguard Design

The origins of safeguard design within the nuclear weapons industry do not stem from a very specific discernable procedure. The earliest evidence uncovered as part of this literature review was National Security Action Memorandum No. 160, issued by President Kennedy on June 6, 1962. This memorandum does not provide a great level of thought regarding two-person control, but it refers to an attachment penned by Jerome Wiesner, chair of the President's Science Advisory Committee.[102]

The topic of the attached memorandum was the permissive action link (PAL) used in nuclear weapons operated by NATO members. These PAL systems were designed to create safeguards to prevent unwarranted use of nuclear weapons. The four objectives of PAL as listed in Wiesner's attachment are:

> (1) Safeguarding weapons against actions by an individual psychotic;
> (2) Meeting the legal and political requirements of U.S. control;
> (3) Maintaining control against the unauthorized use of weapons by our own or allied military forces under conditions or high tension or actual military combat;
> (4) Assuring that weapons could not be used, if forcibly seized by an organized group of individuals or by a foreign power.[102]

These objectives all point toward a means of ensuring control of a nuclear weapon against theft, malicious mischief or zealotry from a lone individual or a group. Wiesner wanted to expand research into PAL controls to ensure that American weapons were not used without specific intent and verification by another trusted agent.

A report by Sandia National Laboratories from 1973 follows up on the use of PAL in nuclear weapons. This document recites some of the history regarding the use of PAL, which sheds insight into how early iterations of nuclear weapons functioned. For example, the report states that device codes operated on a split-knowledge concept, which meant that, "for the purpose of recoding, one man would set in half the code while another would set in the other half."[103] In the case of combination locks, "a five-digit lock was developed to allow the first two combinations and the last two always to be separated by a commonly known integer which would be seen by both men during recoding."[103]

This report describes some of the pieces of control equipment in PAL systems. Several of the systems permit the two-man concept for the purposes of locking and unlocking the PAL device, and recoding the devices permit using the two-team concept.[103]

The Brookings Institution released a comprehensive study titled, "Managing Nuclear Operations."[104] The study notes that the PAL concept appeared as early as 1958, and that weapons utilizing an early version of PAL used standard dual combination locks. These locks require two separate codes to manipulate a nuclear weapon. Manipulation via combination locks for access evolved into manipulation via electromechanical, remote-controlled locks that required a separate portable box to attach to the device finally allowing a two-person team to insert dual codes for access.[104]

One interesting point the study notes is that naval nuclear weapons did not, as of the study's publication in 1987, utilize the PAL concept on submarine-based nuclear weapons. The determined chances of an accidental launch were minimal due to the significant number of people on board the submarine required to take part in the launch process. Safeguards designed into launching procedures include the announcement to the entire crew that the submarine received launch orders, which were subsequently verified by two teams of officers not including the commanding officer, weapons officers or navigator. Following verification, launch keys possessed by crewmembers not included in the launch sequence were given to those responsible for different parts of the launch sequence so the keys could physically manipulate switches in the proper sequence.[104]

Figure 11. "No Lone Zone" sign from missile silo[105]

Since at least 1993 (because repeated updates to instructions since 1993 up to its latest iteration in 2016 continually repeat these requirements), the United States Air Force has instructed personnel charged with safeguarding nuclear weapons in Air Force custody to abide by a "Two-Person Concept" enacted to ensure that one person cannot tamper with a nuclear weapon, system or component in an incorrect or unauthorized manner.[106; 107]

Personnel charged with a nuclear weapons mission must identify no-lone zones (Figure 11), where personnel are not permitted to enter alone and must enter with at least two people authorized for entry. For these areas requiring two people, criteria set forth by the Air Force dictate that each person working on nuclear weapons must (1) be certified via the Personnel Reliability Program, (2) possess knowledge of the nuclear surety tasks they perform, (3) possess the ability to quickly detect incorrect or unlawful acts or procedures, (4) complete Air Force nuclear surety training and (5) be designated to perform the task.

These criteria ensure that personnel know required and expected work procedures, are designed to actually perform the work, and are found to be reliable people.[106; 107]

One major development in the wording of this document not found in the previous report sponsored by the Naval Surface Weapons Center is a requirement for each person inside a no-lone zone to be able to detect incorrect or unlawful acts or procedures. Simply observing a person conducting work on or around a nuclear weapon was no longer enough of a safeguard.

4.7.3 Preventing Human Compromise

On an institutional scale, President Truman recognized the incredible magnitude of destruction nuclear energy could bring and wanted to ensure that nuclear research was regulated by the federal government. At issue was identifying the regulatory body. The military sought to regulate nuclear research, while many nuclear researchers of the time wanted to ensure that scientists would be able to conduct more open research, complete with scientific exchange. Ultimately, President Truman signed into law the Atomic Energy Act of 1946, which established the Atomic Energy Commission (AEC). This act ensured that one entity, the military, was not capable of unilaterally developing weapons for a singular purpose and that nuclear energy was the subject of research and not exclusively war. In order to further develop nuclear weapons, then, the Department of War (predecessor to the Department of Defense) would require input, development and verification from the civilian AEC. President Carter established the Department of Energy in 1977, which assumed the responsibilities and objectives of the AEC and currently maintains control of the nation's nuclear stockpile and research.[108]

Access to nuclear weapons and ability to manipulate, perform work or activate, is highly regulated. Several Department of Defense and Department of Energy documents outline the safeguard designs implemented for nuclear weapons and components, as well as the extensive measures to prevent unauthorized access through reliability programs.

A report sponsored by the Naval Surface Weapons Center (NSWC) in 1979, for example, says that the NSWC uses the "Two-man rule for access to nuclear material" and other measures such as "Personnel reliability program," "Control of access authority," and "Use of exchange badges for exclusion areas."[109] This document is an early review of security procedures from the military regarding nuclear weapons safeguards and security, and all subsequent documents found as part of this literature review require, in essence, at least similar criteria for access to nuclear weapons.

The Air Force's 39th Wing wrote a document called Commander's Guide to Nuclear Surety and Explosives Safety that summarizes many of the criteria from above.[110] In addition, the Department of Defense's unofficial Nuclear Matters Handbook specifies, "The first and most important aspect of procedural security is the two-person rule, which requires the presence of at least two cleared, PRP- or HRP- [human reliability program] certified, and task-knowledgeable individuals whenever there is authorized access to a nuclear weapon."[111] Clearly, the theme of reliable personnel with knowledge of the task and approved access to the material is a best practice in the nuclear industry.

An International Atomic Energy Agency (IAEA) report recommends the use of escorts for work on nuclear weapons. These escorts, according to the recommendations, should "know about their approved activities, including access to specific places and actions they should not perform."[112] The report recommends that team members working with the "two-person rule" should switch between each other, as to reduce complacency. The report further recommends that the transfer of tools and equipment used should be transferred in a more formal manner, with more than one person involved to minimize the insider threat opportunity.[112]

Figure 12. Two Pantex technicians work on a nuclear warhead[113]

Several published Department of Energy policies detail the use of two-person control as related to nuclear weapons, such as Department of Energy Order 452.2D, Nuclear Explosive Safety and Manual 452.2-1A, Nuclear Explosive Safety Manual.[114; 115] The Department of Energy Manual states that the "two-person concept (TPC) is implemented to ensure no lone individual has unrestricted access to a nuclear explosive."[115] As its military counterparts require, the Department of Energy also requires that personnel working with nuclear explosives are subject to a reliability program, authorized for access to the area, knowledgeable about performed tasks and safety requirements, and able to detect incorrect or unlawful acts (Figure 12). The Manual describes how to implement zone coverage for two-person control, as well as person-to-person coverage.[115]

The nuclear weapons industry extensively utilizes reliability programs, and designs systems which require multiple parties to perform separate functions on nuclear systems. These requirements are heavily regulated.

4.8 Biosecurity Industry

4.8.1 Threat to an Asset

The Centers for Disease Control and Prevention, National Institutes of Health, military research laboratories, national laboratories, and research universities actively store dangerous biological agents. Examples of such agents include anthrax, Ebola, plague, and various flu strains.[116; 117]

Accidents can occur in any laboratory. Unlike several of the previous industries reviewed, a mishap with biological agents can have deadly consequences beyond simply the asset's loss. The Centers for Disease Control and Prevention suffered laboratory oversight failures, which led to public disclosures of a lost box containing a deadly virus strain, a recently arrived, label-less package with biological samples in a broken tube, and other workplace safety concerns including potential exposures to biological agents. While workplace safety is a concern, an employee's potential exposure means that a biological agent can

jump from host-to-host to allow easy, possibly undetected access outside of a controlled laboratory setting.[116; 118]

In addition to workplace safety concerns, the insider threat of employee theft remains within the biosecurity industry. An example of this insider threat include the facts surrounding Bruce Ivins, reviewed later in this section, suspected of stealing anthrax from a military laboratory, only to send it via mail to federal officials and news media outlets, killing five people. More instances of the insider threat manifest themselves, including the arrests of individuals for stealing biological agents from different laboratories in separate incidents.[119; 120] In one instance, a researcher knowingly left Canada's high-security research facility, National Microbiology Laboratory (see Figure 13), with twenty-two vials of the Ebola virus on January 21, 2009. The National Microbiology Laboratory is part of Canada's Public Health Agency and conducts research on the most dangerous and infectious biological strains on the planet.[120-122]

With obvious implications to public health, uncontained biological agents represent a significant threat to the biosecurity industry.

Since the federal government regulates access to many harmful biological agents, a lot of practices within the biosecurity industry are designed for two-person control, in which safeguard designs and preventing human compromise assist the practice. An interesting note for this industry, however, is that a large portion of biological research takes place in a purely academic environment, outside the strict structure of military command, and is conducted by trained scientists with academic backgrounds. This leads to friction caused by strict regulation conflicting with a desire for academic freedom.[123] As will be reviewed, this facet of biosecurity brings about issues with implementing safeguard designs through institutional push-back against strict adherence to two-person control.

4.8.2 Safeguard Design

The biosecurity industry appears to be at a crossroads with implementing two-person control safeguard designs. While it is seen as beneficial to counter the insider threat, the safeguards themselves are considered a burden to researchers and staff who are not comfortable with working in a security-based environment. As will be reviewed, the adoption of two-person control safeguards is rising within the industry, but not without practitioner pushback. For the safeguard designs the industry does implement, it tends to prefer engineered implementations over human implementations.

Researchers with the U.S. Army Medical Research Institute of Infectious Diseases studied the implementation of biosurety systems in a Defense Department laboratory. The researchers wrote that the two-person rule, as used in the laboratory setting, is an accountability measure of the Department of the Army and is more flexible than other military settings, such as those regulating chemical or nuclear materials. For example, the use of video surveillance or "roving observation of laboratory activities"[15] is preferred over another person physically standing near another. The study notes that the fiscal cost of implementing two-person control, as used in the chemical or nuclear weapons settings, was very high and that laboratory settings are too small to accommodate multiple people comfortably.[15]

A Defense Science Board Task Force (DSBTF) reported to the Under Secretary of Defense on the Department of Defense Biological Safety and Security Program. This May 2009 report reviews how the two-person rule is implemented within a biological program's setting. One of the findings states that video monitoring in the laboratory setting can be superior to a two-person rule with regard to detection and deterrence. As well, transporting assets using a two-person rule could be potentially worse than a "lost in the crowd" approach, in which a multitude of items are moved around or shipped every day.[124]

Surprisingly, however, the report states that implementing the two-person rule for the laboratory setting is a potential improvement to counteract the insider threat. The report continues, though, that the rule is considered "onerous," costly and physically dangerous for the second person. The report argues that the use of two-person control for monitoring purposes is "counter-productive" and lowers employee morale by treating everyone "as a suspect."[124]

Figure 13. National Microbiology Laboratory in Winnipeg, Manitoba[121]

The National Science Advisory Board for Biosecurity (NSABB) released reports regarding two-person control in biological laboratories in May 2009, and September 2011, after the suicide of Army researcher Bruce Ivins, the Federal Bureau of Investigation's suspect in the 2001 anthrax mailings. Safeguard designs are not categorically rejected by biosecurity practitioners, though. The NSABB repeatedly rejected calls to mandate the rule for laboratories. By noting the "General lack of support" for implementing two-person control, the NSABB considers the measure one to not implement at smaller laboratories with a smaller workforce but recommended that individual institutions make their own determinations on which safeguards, if any, to implement.[123; 125] This very much compares to European civil aviation regulators' decision to allow individual airlines to determine whether or not to require two pilots in the cockpit on a flight.

The NSABB noted in its September 2011 report that safeguards are employed to enhance, in part, biosecurity in the high-containment laboratory environment.[125] Practitioners and the NSABB advisory board appear to favor safeguards primarily for assets determined to be dangerous enough to require safeguards. Safeguard designs for low-level biological agents appear to be the source of contention between security and research considerations.

Kavita Berger, however, wrote an article for the American Association for the Advancement of Science's *Science* magazine touching upon safeguard designs found within life science laboratories. Berger notes that safeguard designs, including, "key card or biometric controls, gates, security guards, security cameras, and training" might appear "draconian" to the researcher, however, these practices are in place at many research institution as security measures.[126] As the article notes, "Although the overall number of cases is low, harmful acts continue to take place, which suggests the need to develop and implement systems to identify and stop incidents from occurring at the individual, institutional, community, and federal levels."[126] Life science laboratories acknowledge a risk to their facilities, yet hesitantly implement safeguard designs.

Efforts to increase safeguard designs are evident. For example, the National Center for Biotechnology Information, part of the National Institute of Health, dedicates a webpage to laboratory security with recommendations made by the National Research Council Committee on Prudent Practices in the Laboratory. This publication, free for online reading and also available in hardcopy, describes the reasons for implementing safeguards, methods of engineered implementations through physical and electronic security, and human implementations through visual and operational security methods.(127)

4.8.3 Preventing Human Compromise

The National Science Advisory Board for Biosecurity's May 2009 report reviews personnel reliability requirements for employees with access to certain biological agents. While the report notes a lack of support among the scientific community for two-person control safeguard designs, it strongly supports the use of reliability programs to check for one's criminal, financial, employment, medical and substance abuse history.(123)

The biosecurity industry uses multiple personnel reliability programs due to multiple biosecurity practitioners each with separate vetting processes. For example, the biosecurity industry in the United States performs work in laboratories owned by private organizations, hospitals, government, and universities. Laboratory owners have different personnel reliability methods.

One personnel reliability program researchers working with dangerous biological agents at institutions use is the Security Risk Assessment (RSA). The RSA requires a "basic FBI [Federal Bureau of Investigation] background check," as one article notes, which includes submitting one's fingerprints to crosscheck against criminal and terrorist databases.(128) Disqualifiers for a successful SRA completion include a negative criminal history, mental health or substance abuse issues, citizen of a country sponsoring terrorism, and dishonorable discharge from the military. The SRA, as of 2009, took less than two months to complete and was valid for five years.(128)

The FBI does not fully endorse SRAs as a foolproof vetting program, as it only checks on already documented information with which to vet somebody. As one article notes, "experts point out it is a fairly limited form of vetting."(128) A government-sponsored security clearance, in contrast, considers a person's entire life background, including social connections, and not just records checks. The article makes a note of Lawrence Livermore National Laboratory's (LLNL) use of such security clearances to vet employees working with biological materials. In addition to this security clearance, biological laboratory managers at LLNL must have "extensive conversations with past managers"(128) to determine an employee's temperament. As well, these employees are psychologically evaluated on an annual basis. The drawback to such measures, notes the select agent manager at LLNL, is that very talented researchers who come to work at LLNL "suffer a rude shock," making employee retention difficult.(128)

The NSABB released another report in September 2011 (previously referenced) regarding the culture of responsibility as it relates to enhancing personnel reliability. This report repeats several findings from the Board's previous report mentioned above, stressing records checks and fingerprint database inquiries. The report recommended that the two-person rule not be federally mandated, but should be implemented as determined by each laboratory following a risk assessment. The report does not qualify what exactly is meant by risk assessment with regard to a culture of responsibility.(125)

As mentioned above, Bruce Ivins was an insider threat to the biosecurity industry. Following successful completion of a reliability program that provided Ivins with the necessary security clearance and access to biological agents, Ivins circumvented two-person control implementations at an Army research facility in Fort Detrick, Maryland. The FBI suspects that Ivins stole strains of anthrax from the U.S. Army Medical

Research Institute of Infectious Diseases and then sent them in the mail to Senators Leahy and Daschle, as well as to news media outlets, killing five people and injuring seventeen.[128-130]

While this literature review found documents suggesting that two-person control was in place at Fort Detrick at the time of Ivins' employment, the trend within the biosecurity industry suggests the implementations were not as formal or "onerous," as it has been called, as other industries safeguarding very deadly assets. One would have to review the extent of Fort Detrick's safeguard designs to compare implementations with other industries within the military apparatus, such as chemical or nuclear weapons, to determine if two-person control methods were effectively implemented.

While the biosecurity industry uses a reliability program to prevent unauthorized access to its assets, safeguard designs are met with a significant amount of resistance. The industry appears to worry about the insider threat, but does not consider the need for additional oversight as especially productive to research. This is, in part, due to researchers feeling impeded by oversight and unable to conduct open research. Academics suggested that rather than implementing safeguard designs to enforce two-person control, lab managers should be trusted to manage their employee's action. For example, Stony Brook University simply requires rooms to be locked when unoccupied, but allows lab users to "use judgment in providing keys to visitors," only disallowing lone visitor access when in a laboratory with a higher security level.[131]

Worth noting in response to limited safeguard measures within a laboratory, however, is the instance of a researcher's January 2009 theft of the Ebola virus from the National Microbiology Laboratory, briefly mentioned above, where "senior lab officials admitted they had no idea that 22 vials of biological substances were missing from the high-security facility for close to four months." Laboratory officials only came to discover the Ebola vials were missing upon the researcher's arrest in early May 2009, at the Canada-United States border by United States customs officers, who discovered the vials in the trunk of the researcher's vehicle. The researcher, Konan Michael Yao, told United States customs officers that he wanted to take his work to his new job at the National Institutes of Health at the Biodefense Research Laboratory in Bethesda, Maryland, so he didn't have to start his research all over again.[120; 122]

4.9 Summary of Modern Industry

Parsing two-person control practices by the three elements used throughout this section, a review of modern industries shows that industry threats and practices slightly differ within the elements of identified threat and preventing human compromise, but practices most notably differ with regard to the safeguard design element. Identified threats vary across the reviewed industry, with the sole exception of the insider threat. For example, assets facing threats ranged from casino chips to airplane cockpits, but the insider threat remained. Methods of preventing human compromise stem from ensuring an organization employs a reliable employee. Evidence of this was seen as far back as the late-nineteenth century as reviewed in Section 3, and is seen in modern industry by every reviewed industry relying on some form of employee reliability or credentialing program.

Safeguard design most notably differs by virtue of each industry's manifestation of safeguard designs. For example, assets requiring protection are not identical, as assets range from items secured in vaults to items secured while in transport to digital access to computer networks. Safeguard design more notably differing between industries than the other two elements is almost expected when one considers that the asset requiring safeguard will not always be the same. However, an industry can more responsibly identify threats to its assets and methods of preventing human compromise than duplicate engineered or human-based manifestations of safeguard design as an immediate safeguard solution. Consider, again,

that a casino gaming chip requires different safeguard designs than does an airplane cockpit, but methods of preventing human compromise to both overlap through employee reliability programs.

Table 1 quickly summarizes each industry as it relates to one of the three identified elements.

Industry	**Element 1** **Identified Threat**	**Element 2** **Safeguard Design**	**Element 3** **Preventing Human Compromise**
Financial	• Money • Safe deposit boxes • Insider threat	• Segregation of duties • Internal controls • Banking operations	• Organizational liability • To prevent the hiring of "dishonest" employees
Information Technology	• Networks • Databases • Industrial operations • Insider threat	• Role-based access control • Secret sharing	• Reliability primarily through certifications • Developing methods of ensuring proper access
Civil Aviation	• Hijacking • Intentional crashing • Insider threat	• Two pilots in the cockpit is not yet universally required, but still implemented as best practice	• Mental health screening • Cockpit door security
Gaming	• Money • Chips • Insider threat	• Vaults • Surveillance methods • Access control • Dual concurrence	• Personnel reliability programs • Criminal, financial, social, mental health checks
Pharmaceutical	• API • Offsite distribution • Insider threat	• Federal oversight • Vaults • Surveillance methods • Dual concurrence • Auditing and accountability	• "Halo effect" for vetted employees • Employee blacklists • Deliveries to offsite vendors have no safeguards
Chemical Weapons	• State and non-state actors • Insider threat	• Access control • Storage methods • Pre-defined transportation requirements	• Personnel reliability programs (PRP) • "Emotional and mental stability, trustworthiness, physical competence, and adequate training"
Nuclear Weapons	• Theft • Damage • Intentional activation • Insider threat	• PAL • Submarine launch sequence • No-lone zones	• Atomic Energy Act of 1946 • PRP/HRP
Biosecurity	• Theft • Cascading accidents • Insider threat	• Video monitoring • Industry pushback	• Reliability programs

Table 1. Element summaries for each industry reviewed

5. A THEORY ON HOW TWO-PERSON CONTROL ENTERED MODERN INDUSTRY

This research earlier reviewed instances of two- and multi-person controls as they appeared throughout history in documents and facts uncovered from reviewing open source literature. A literature review on the topic uncovered exclusively Western sources and histories of the practice. While this was not intended, research into the topic originating from non-Western sources simply did not appear. Perhaps more focused and specific research would uncover other historical instances of two- or multi-person control to assist in understanding its origin – instances older than the ancient Roman practice that saw a king's power vested into dual praetors.

The American military has existed since before the American colonies claimed independence from the British Empire in 1776. However, antiquated documents from this time period specifying two-person controls for safeguarding military assets were not uncovered as part of this literature review. Perhaps documents such as these exist, but this review happened to not come across them. The only documents uncovered regarding two-person control in the American military related to the handling of more modern chemical, biological, and nuclear assets.

From the evidence found as a result of this literature review, two-person control for asset protection emerged at least as early as the mid-nineteenth century with regard to safeguarding money and other high-value assets left in the charge of financial institutions. The financial industry, specifically safe deposit box companies, made efforts to implement safeguard designs and prevent unauthorized access for the primary purpose of liability. The few instances discovered as part of this literature review in which this liability was tested in court found that the companies made points in either their contractual obligations or briefs to the court that they purposefully implemented two-person control safeguards and prevented unauthorized access, demonstrating that companies were proactive in efforts to implement two-person control. In fact, the safe deposit box companies were so proactive in their efforts that they recommended implementing such measures as an industry best practice as early as 1904.

At some point in time, between 1914 and 1962, practices of two-person control entered into industries outside of finance. Other than the financial industry and the military, all industries reviewed in this paper did not exist in their current forms at the turn of the century, and as mentioned, no documents for the military with regard to two-person control for asset protection were uncovered for a period prior to 1962, with National Security Action Memorandum Number 160. This lack of documentation leads to a gap in fully understanding how two-person control entered into other industries. Certainly, the elements are present, but the motivations are unclear.

One theory of how two-person control was implemented in industries other than finance is that industries protecting high-value assets observed how the financial industry took measures to safeguard its property using the three previously-defined elements: an asset faces a threat, an implementation requiring two people for access to an asset exists, and the organization works to prevent unauthorized access. The financial industry had a long and documented history of safeguarding its assets through the use of safeguard design implementations and the hiring of reliable employees.

How could the gaming industry, for example, overlook how bank vaults store, control access to, and safeguard high-value assets? Is bank-like security not exactly what the gaming industry sought to accomplish with asset protection? Does an organization with responsibility for civil aviation, such as the FAA, want to ensure that airplanes are only flown by dependable and competent pilots who won't intentionally crash an airplane, much like financial institutions want to only hire dependable and competent employees who won't intentionally steal from the bank? Would not the guardians of nuclear

weapons want to ensure that one person does not have sole access to a nuclear weapon's launch capability, just as the financial industry recommended in 1904 that one employee locking a vault should not know the pre-set time on the time-lock the other employee set, thereby limiting the possibility of unauthorized access?

Each industry reviewed takes measures to address the three elements of two-person control introduced toward the beginning of this review. Each industry protects an asset, implements safeguard designs to enforce the need for two people to be involved with access to an asset, and each industry prevents unauthorized access to its asset. But do any of the industries reviewed analyze two-person control as practiced in its own industry?

While the information technology industry adapted safeguard designs to assets in a digital plane, this review found no indication that any reviewed industry formally considered important questions: Why are we using two-person control to safeguard our assets? Will two-person control adequately safeguard our industry's assets from the threats they face? Do another industry's two-person control implementations already provide the best safeguard solution for our industry's assets? Industry practitioners to fully consider these types of questions would provide a safeguard solution tailored to address specific needs custom to their industry.

Two-person control not only serves to protect physical assets in a locked safe, but creates a framework for protection of any asset. Many of these industries have faced threats and needed to change the practices by which they safeguard their assets, which is how the conceptual framework of two-person control allows multiple industries to implement it.

Evidence of a two-person control framework is found in the similarities between the information technology industry, for example, and the nuclear industry. One can note the similarities between the ISE-T study, in which actions must be duplicated in order for the action to be validated, and work performed in the nuclear weapons industry, in which one must be knowledgeable of actions to take and able to quickly detect any incorrect actions another takes. In both cases, actions must be validated by another. Work validation is shared in other industries, as well, including the gaming and pharmaceutical industries.

Two-person control across an entire industry is not implemented overnight. Consider the Great Gold Robbery of 1855. Two elements of two-person control were in place – safeguard designs and preventing human compromise – but the South-Eastern Railway Company did not appear to fully consider the extent of the threat to the gold coming from its own employees, the insider threat. Still, the financial industry learned from events like these to implement more stringent requirements for asset protection. Just as the financial industry eventually developed into a very regulated industry implementing two-person control, newer industries reviewed are currently learning how to most effectively implement these safeguards. Consider the biosecurity industry's pushback to unfavorable security measures despite the reluctant adoption of them. The documented history of two-person control as a success story and safeguard tactic, however, suggests that its framework is any industry's best practice for safeguarding assets.

Civil aviation is becoming ever more reliant on safeguarding measures offered by two-person control. Like the biosecurity industry, civil aviation is newer to the safeguarding concept, but is critically dependent on it. Successfully implementing new safeguards takes time and policy iterations to identify and resolve gaps and other considerations. For example, screening and monitoring of all passengers only became fully federally regulated through the creation of the Transportation Safety Administration (TSA) shortly after September 11, 2001. Even with nearly fifteen years in existence, the TSA allegedly still has issues identifying the threats it was established to screen out, as demonstrated by TSA screening practices not properly identifying ninety-five percent of breach tests.[132]

The timeline below (Figure 14) represents topics covered as part of this literature review regarding two-person control. Note the earliest documented instances are from the financial industry. After a lull of two generations, two-person control begins to emerge within the nuclear weapons industry. Finally, note the obvious increase in literature, discussions, and instances regarding two-person control beginning in 1987 to the present day (YTD).

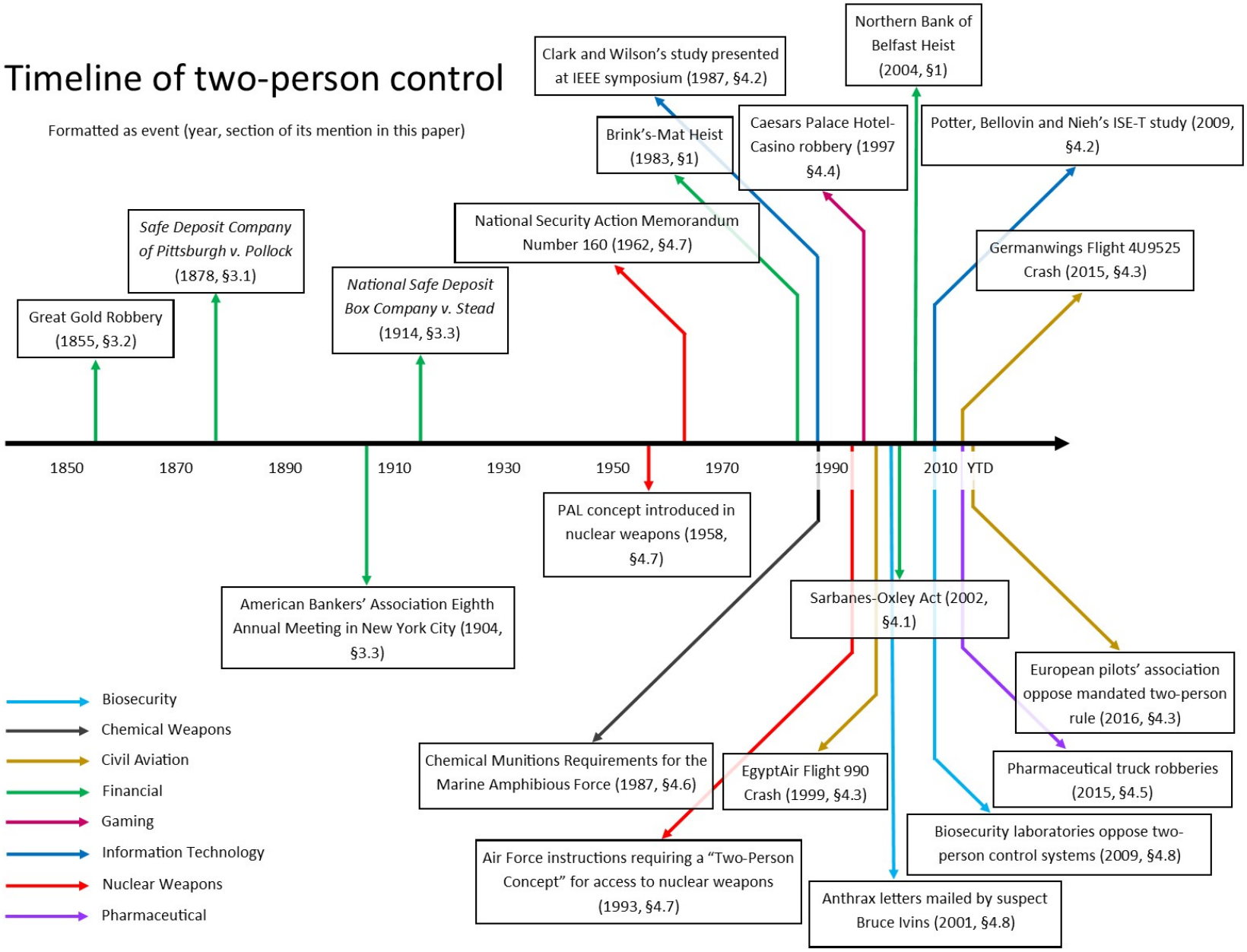

Figure 14. Timeline of events documented in this review regarding two-person control

6. CONCLUSION

The history surrounding two-person control is one of constant evolution. Companies did not introduce the practice overnight. As demonstrated, the practice began in a rudimentary fashion, but in one instance was defeated by determined criminals in the mid-nineteenth century. The practice eventually evolved into a much more detailed and regulated system. Much of this evolution was not uncovered during the course of this literature review, however. Private companies are not required to publish internal policies for asset protection. Even more, a private company might not even have documents related to asset protection policies from over a century ago. As research continues and becomes more prominent into the topic of two-person control, perhaps a corporate historian will recognize the significance of antiquated company policies.

Perhaps the greatest advantage of implementing two-person control is to combat the insider threat. As seen in Table 1, the insider threat is an identified threat in every single industry, the only shared threat between all industries reviewed. With two-person control, an employee becomes a trusted agent through the vetting of a reliability program that screens for obvious employer concerns prior to providing an employee access to an asset. These employer concerns, again, can include a negative employment history, financial misfortunes, an undesirable criminal history, drug abuse history, unsavory social ties and mental health issues. Even with such screening, an employee is still subject to safeguard designs such as requiring another employee to verify actions taken or unlock a room for access to an asset. Unilateral access or manipulation is not permitted.

Two-person control measures have still been defeated, though, due to the insider threat, as seen in the Brink's-Mat incident. This does not mean that two-person control does not work. Quite the opposite, in fact. Industries that do not rely on the implementations of two-person control open themselves up even wider to liability and the insider threat. In fact, it would be impossible to determine how many insider acts have been institutionally thwarted by existing two-person control implementations due simply to the fact that the acts did not occur.

The future of two-person control is expansive. A 1991 report considered the ways in which a biometric access system could support a two-person rule in certain rooms within a secure facility.[133] In the 2008 study reviewing the ISE-T system, an information technology system administrator's verification system allowed for an infinite number of cloned systems. Once modified, an unverified modification could be automatically wiped out through a restart of the cloned system.[58] This example represents a recent expansion of two-person control that demonstrates the flexibility of its conceptual framework.

Two-person control started in the physical realm. A look at the history of two-person control over the past one hundred and fifty years shows that the practice has received a lot of attention in one form or another starting in the late 1980s. If this exposure is an anomaly due to media coverage or some other coincidence, the pattern has not subsided for nearly thirty years. As such, two-person control is now a best practice in several industries.

With regard to the future of two-person control, the growing trend in preventing human compromise points to adopting a standard of two-person control practitioners possessing similar training and experience, or other forms of shared qualifications. The ultimate methods an organization is willing to employ in order to negate with complete confidence the actions of a compromised employee are yet to be determined, however. As well, considering the ever-expanding development and integration of information technology systems with everyday life, the application of two-person control in the digital realm appears to be the next frontier in two-person control safeguard design.

REFERENCES

1. McGuinness, Ross. "Brink's-Mat: 30 years on from Britain's most notorious gold robbery." (2013). Available: http://metro.co.uk/2013/11/22/brinks-mat-30-years-on-from-britains-most-notorious-gold-robbery-4196170 [Sep 20, 2016].
2. "Brinks Mat gold: The unsolved mystery." *BBC News* (2000). Available: http://news.bbc.co.uk/2/hi/uk_news/714289.stm [Aug 30, 2016].
3. Coates, Sam. "Whatever happened to Brinks-Mat?" *Independent* (1996). Available: http://www.independent.co.uk/arts-entertainment/whatever-happened-to-brinks-mat-1353688.htm [Aug 31, 2016].
4. Feder, Barnaby J. "Guard Gives Details of British Gold Robbery." *The New York Times* (1984). Available: http://www.nytimes.com/1984/02/18/world/guard-gives-details-of-british-gold-robbery.html [Aug 30, 2016].
5. Roper, Matt. "Fool's Gold: The curse of the Brink's-Mat gold bullion robbery." Mirror, 2012. Available: http://www.mirror.co.uk/news/uk-news/the-curse-of-the-brinks-mat-gold-bullion-robbery-829220 [Sep 30, 2016].
6. "Timeline: Northern Bank robbery." *BBC News* (2005). Available: http://news.bbc.co.uk/2/hi/uk_news/northern_ireland/4117219.stm [Aug 31, 2016].
7. "Northern Bank Robbery." *Crime File*. Crime Investigation Network. 2015. Available: http://www.crimeandinvestigation.co.uk/crime-files/northern-bank-robbery/crime.html [Aug 31, 2016].
8. "Ward walks free as £26m bank robbery trial collapses." *Belfast Telegraph* (2008). Available: http://www.belfasttelegraph.co.uk/news/ward-walks-free-as-26m-bank-robbery-trial-collapses-28450027.html [Aug 31, 2016].
9. "10 facts about the IRA's £26.5m raid on Northern Bank." Belfast Telegraph, 2014. Available: http://www.belfasttelegraph.co.uk/news/northern-ireland/10-facts-about-the-iras-265m-raid-on-northern-bank-30848746.html [Oct 31, 2016].
10. Hamilton, Alexander, John Jay, and James Madison. *The Federalist*. New York: Random House, 2001. Print.
11. History.com. "Magna Carta." 2009. Available: http://www.history.com/topics/british-history/magna-carta [Oct 4, 2016].
12. Abbott, Frank F. *A History and Description of Roman Political Institutions*. Boston: Ginn & Company, 1901. Print.
13. Cicero. *Cicero: Selected Letters*. Trans. Walsh, P.G. Oxford World's Classics: Oxford University Press, 2008. Print.
14. Rio Tinto, Daniel. "Renewed calls to enforce a "two-person rule" on flight decks after Germanwings crash." (2015). Available: http://phys.org/news/2015-03-renewed-two-person-flight-decks-germanwings.html [Aug 15, 2016].
15. Carr, K., et al. "Implementation of biosurety systems in a Department of Defense medical research laboratory." *Biosecur Bioterror* 2.1 (2004): 7-16. https://www.ncbi.nlm.nih.gov/pubmed/15068675.
16. Cappelli, Dawn, Andrew Moore, and Timothy Shimeall. *Common Sense Guide to Prevention and Detection of Insider Threats*: US-CERT, 2005. Print.
17. "The History of the Safe Deposit Box." Metropolitan Safe Deposits. 2016. Available: http://www.metrosafe.co.uk/editorials/news-releases/date/2016/03/01/the-history-of-the-safe-deposit-box/ [Jan 17, 2017].
18. Cummins, Jr., Thomas K. "A Review of the Law of Safe-Deposit Companies." *Harvard Law Review* 9.2 (1895): 131-43. http://www.jstor.org/stable/1322128.
19. The Safe Deposit Company of Pittsburgh v. Pollock. Supreme Court of Pennsylvania 1878.
20. "Longmont, Col., July 18, 1889." *The Banking Law Journal* 1.1 (1889): 196-7.
21. Morley, Stephen. "Historical UK inflation rates and calculator." n.d. Available: http://inflation.stephenmorley.org/ [Aug 30, 2016].
22. "The Story of a Great Bullion Robbery." *Chambers's Journal* 2 (1898): 109-12.
23. Evans, D. Morier. *Facts, Failures, and Frauds: Revelations, Financial , Mercantile, Criminal*. London: Groombridge & Sons, 1859. Print.
24. Nash, Jay R. *The Great Pictorial History of World Crime*. Vol. 2. London: First Rowman & Littlefield, 2014. Print.
25. "The Great Gold Robbery, 1855." British Transport Police, n.d. Available: http://www.btp.police.uk/about_us/our_history/crime_history/the_great_gold_robbery,_1855.aspx [Sep 30, 2016].
26. "Report of Special Trust Company Committee on Legal Decisions Relating to Safe Deposit Companies." *American Bankers' Association*. 1904. Print.

27. National Safe Deposit Company v. Stead, Attorney General of the State of Illinois. Supreme Court of the United States 1914.
28. Fernandes, Deirdre. "The disappearing allure of the safe deposit box." The Boston Globe, 2014. Available: ttps://www.bostonglobe.com/business/2014/03/08/the-disappearing-allure-safe-deposit-box/HvwkPkvAUtoo8329bZrKsM/story.html [Jan 17, 2017].
29. "Bank Crime Statistics 2014." Federal Bureau of Investigation: Justice, Department of. 2015.
30. "Risk Management Manual of Examination Policies." Corporation, Federal Deposit Insurance. 2015.
31. *A risk-based approach to segregation of duties*: Ernst & Young, 2010. Print.
32. Hanna, Julia. "The Costs And Benefits Of Sarbanes-Oxley." *Forbes* (2014). Available: http://www.forbes.com/sites/hbsworkingknowledge/2014/03/10/the-costs-and-benefits-of-sarbanes-oxley/#34f52af62776 [Jan 17, 2017].
33. Van, Jon, and Alexander Delroy. "Andersen was WorldCom Auditor." *Chicago Tribune* (2002). Available: http://www.chicagotribune.com/sns-worldcom-andersen-ct-story.html [Jan 20, 2017].
34. Tkaczyk, Christopher. "The 10 largest U.S. bankruptcies." *Fortune* (2009). Available: http://archive.fortune.com/galleries/2009/fortune/0905/gallery.largest_bankruptcies.fortune/3.html [Jan 20, 2017].
35. *Internal Control - Integrated Framework*: Committee of Sponsoring Organizations of the Treadway Commission, 2013. Print.
36. "Opening Procedures." Money Business Services. 2016. Available: http://moneyservicesbusiness.com/risk-mgt/opening-procedures/ [Sep 8, 2016].
37. "Closing Procedures." Money Business Services. 2016. Available: http://moneyservicesbusiness.com/risk-mgt/closing-procedures/ [Sep 8, 2016].
38. "Dual Control." Money Business Services. 2016. Available: http://moneyservicesbusiness.com/risk-mgt/dual-control/ [Sep 8, 2016].
39. Marx, Claude R. "Opening- and Closing-Time Robberies Can Be Especially Devastating." *Credit Union Times Magazine* (2009). Available: http://www.cutimes.com/2009/06/03/opening-and-closingtime-robberies-can-be-especially-devastating [Jan 20, 2017].
40. Tuttle, Beecher, and Dan Butcher. "Everything you need to know about pre-employment background checks." efinancialcareers. 2016. Available: http://news.efinancialcareers.com/us-en/150222/everything-you-need-to-know-about-pre-employment-background-checks/ [Jan 16, 2016].
41. Lum, Zi-Ann. "Use Of Credit Checks To Screen Job Applicants Growing In Canada As U.S. Clamps Down." (2015). Available: http://www.huffingtonpost.ca/2015/04/21/td-bank-credit-rating-jobs_n_7057312.html [Jan 16, 2017].
42. "Bank Robberies." Federal Bureau of Investigation. 2016. Available: https://bankrobbers.fbi.gov [Sep 8, 2016].
43. Parsons, Kye. "Bank Employees Arrested for Stealing." (2008). Available: http://www.wboc.com/story/8215268/bank-employees-arrested-for-stealing [Sep 8, 2016].
44. "Wells Fargo Workers Allegedly Stole $800k From Dead Customers' Accounts." (2016). Available: http://sanfrancisco.cbslocal.com/2016/02/03/wells-fargo-workers-allegedly-stole-800k-from-dead-customers-accounts/ [2016].
45. Glazer, Emily, and Christopher M Matthews. "Federal Prosecutors Investigating Wells Fargo Over Sales Tactics." *The Wall Street Journal* (2016). Available: https://www.wsj.com/articles/federal-prosecutors-investigating-wells-fargo-over-sales-tactics-1473881424 [Sep 14, 2016].
46. Venezia, Paul. "Sorting out the facts in the Terry Childs case." (2008). Available: http://www.cio.com.au/article/255165/sorting_facts_terry_childs_case/ [Feb 1, 2017].
47. Kravets, David. "S.F. Admin Guilty of Hijacking City Passwords." *Wired Magazine* (2010). Available: https://www.wired.com/2010/04/admin-guilty/ [Feb 1, 2017].
48. "Visualizing the U.S. Electric Grid." (2009). Available: http://www.npr.org/2009/04/24/110997398/visualizing-the-u-s-electric-grid [Jan 20, 2017].
49. "Eastern and Western Interconnection Seams and Optimal HVDC Overlay Study." National Renewable Energy Laboratory: Energy, Department of. 2015.
50. *Results of the SANS SCADA Security Survey*: SANS Institute, 2013. Print.
51. Ball, James. "Meet the seven people who hold the keys to worldwide internet security." (2014). Available: https://www.theguardian.com/technology/2014/feb/28/seven-people-keys-worldwide-internet-security-web [Mar 31, 2017].
52. "DNS and DNSSEC." American Registry for Internet Numbers. Available: https://www.arin.net/resources/dnssec/ [May 3, 2017].

53. Habib, Muhammad Asif. "Role inheritance with object-based DSD." *International Journal of Internet Technology and Secured Transactions* 3.2 (2011): 149-60.
54. *A comparison of commercial and military computer security policies*. Security and Privacy, 1987 IEEE Symposium on. 1987. IEEE. Print.
55. Nyanchama, Matunda, and Sylvia Osborn. "Role-based security, object oriented databases and separation of duty." *ACM Sigmod Record* 22.4 (1993): 45-51.
56. Botha, Reinhardt A., and Jan H. P. Eloff. "Separation of duties for access control enforcement in workflow environments." *IBM Systems Journal* 40.3 (2001): 666-82.
57. Sandhu, Ravi S, and Pierangela Samarati. "Access control: principle and practice." *IEEE communications magazine* 32.9 (1994): 40-48.
58. *Two-Person Control Administation: Preventing Administation Faults through Duplication*. LISA. 2009. USENIX Association. Print.
59. Shamir, Adi. "How to share a secret." *Communications of the ACM* 22.11 (1979): 612-13.
60. "TCR Selection 2010." Root DNSSEC. 2010. Available: http://www.root-dnssec.org/tcr/selection-2010/ [Mar 31, 2017].
61. Dillow, Clay. "An Order of Seven Global Cyber-Guardians Now Hold Keys to the Internet." *Popular Science* (2010). Available: http://www.popsci.com/technology/article/2010-07/order-seven-cyber-guardians-around-world-now-hold-keys-internet [Mar 31, 2017].
62. "Bath entrepreneur 'holds the key' to internet security." (2010). Available: http://news.bbc.co.uk/local/bristol/hi/people_and_places/newsid_8855000/8855460.stm [Mar 31, 2017].
63. *Secure distributed membership tests via secret sharing: How to hide your hostile hosts: Harnessing shamir secret sharing*. Computing, Networking and Communications (ICNC), 2016 International Conference on. 2016. IEEE. Print.
64. Lindros, Kim. "5 Great 'Starter' Cybersecurity Certifications." (2016). Available: http://www.businessnewsdaily.com/9661-cybersecurity-certifications.html [Jan 23, 2017].
65. States, National Commission on Terrorist Attacks Upon the United. *The 9/11 Commission Report*. First ed: W.W. Norton & Compan, Inc., 2004. Print.
66. Campbell, Duncan. "Revenge drove pilot to crash plane, killing 217." (2002). Available: https://www.theguardian.com/world/2002/mar/16/duncancampbell [Sep 1, 2016].
67. "Eight 'pilot suicides' recorded in past 40 years, killing hundreds of passengers, crew and people on the ground." ITV. 2015. Available: http://www.itv.com/news/2015-03-26/eight-pilot-suicides-recorded-in-past-40-years-killing-hundreds-of-passengers-crew-and-people-on-the-ground/ [Sep 1, 2016].
68. Botelho, Greg, and Laura Smith-Spark. "Germanwings crash: Plane obliterated, 150 presumed dead." CNN, 2015. Available: http://www.cnn.com/2015/03/24/europe/france-plane-crash/ [Sep 30, 2016].
69. Kirchner, Stephanie, and Anthony Failoa. "French prosecutor: Co-pilot took doomed flight on deliberate dive." *The Washington Post* (2015). Available: https://www.washingtonpost.com/world/pilot-reportedly-locked-out-of-cockpit-before-plane-crashed-into-alpine-mountainside/2015/03/26/460770d8-d38c-11e4-a62f-ee745911a4ff_story.html [Sep 8, 2016].
70. "Germanwings Flight 4U9525: Canadian airlines told to have 2 people in the cockpit." *CBC News* (2015). Available: http://www.cbc.ca/news/world/germanwings-flight-4u9525-canadian-airlines-told-to-have-2-people-in-the-cockpit-1.3010494 [Sep 1, 2016].
71. Engel, Pamela. "Here's how Airbus cockpit doors work - and why the Germanwings co-pilot was able to lock out the captain." (2015). Available: http://www.businessinsider.com/how-airbus-a320-cockpit-doors-work-2015-3 [Jan 20, 2017].
72. Aratani, Lori, and III Halsey, Ashley. "Security experts say U.S. rules aim to prevent lone-pilot scenario." *The Washington Post* (2015). Available: https://www.washingtonpost.com/national/security-experts-say-us-rules-aim-to-prevent-lone-pilot-scenario/2015/03/26/ee240db8-d3cc-11e4-ab77-9646eea6a4c7_story.html [Sep 8, 2016].
73. "Exemptions, Deviations, Waivers, and Authorizations." Federal Aviation Administration: Transportation, Department of. 2015.
74. "Exemptions, Deviations, Waivers, and Authorizations." Federal Aviation Administration: Transportation, Department of. 2015.
75. Wall, Robert. "U.K. Regulator Asks Airlines to Review Cockpit Rules After Germanwings Plane Crash." *The Wall Street Journal* (2015). Available: http://www.wsj.com/articles/uk-regulator-asks-airlines-to-review-cockpit-occupancy-rules-1427397688 [Sep 1, 2016].
76. *Minimum Occupancy of the Flight Deck (ECA Position Paper)*: European Cockpit Association, 2016. Print.

77. *Summary of survey results on "Assessment of effectiveness of 2-persons-in-the-cockpit recommendation included in EASA SIB 2015-04"*: European Aviation Safety Agency, 2016. Print.
78. Moores, Victoria. "Germanwings crash prompts new medical rules." Air Transport World. 2016. Available: http://atwonline.com/safety/germanwings-crash-prompts-new-medical-rules [Sep 13, 2016].
79. *Opinion 14/2016*: European Aviation Safety Agency, 2016. Print.
80. Sullivan, Tom. "#Germanwings Tragedy: In There Too Much Security on Airplanes?". Fox News Radio, 2015. Available: http://radio.foxnews.com/2015/03/27/germanwings-tragedy-is-there-too-much-security-on-airplanes/ [Jan 20, 2017].
81. de Castella, Tom. "Who, What, Why: How are cockpit doors locked?" *Magazine Monitor* (2015). Available: http://www.bbc.com/news/blogs-magazine-monitor-32070528 [Jan 23, 2017].
82. Bunn, Matthew, and Kathryn M Glynn. "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries." *Journal of Nuclear Materials Management* 41.3 (2013): 4-16.
83. "Caesars Palace Cash Cart Snagged In Armed Robbery." *Orlando Sentinel* (1997). Available: http://articles.orlandosentinel.com/1997-05-19/news/9705190093_1_caesars-security-guards-palace [Sep 20, 2016].
84. Housel, Theodore F.L. "News Release." Jan 15, 2010. Atlantic County Prosecutor's Office. Available: [Jan 12, 2017].
85. Abrams, Jonathan, and David Reyes. "Employee is suspected in casino heist." *The Los Angeles Times* (2007). Available: http://articles.latimes.com/2007/aug/03/local/me-heist3 [Sep 20, 2016].
86. "Controlled Substance Schedules." Drug Enforcement Agency: Justice, Department of. n.d.
87. Lloyd, Sederer. "A Blind Eye to Addiction." *U.S. News & World Report* (2015). Available: http://www.usnews.com/opinion/blogs/policy-dose/2015/06/01/america-is-neglecting-its-addiction-problem [Jan 25, 2017].
88. "Opioids drive continued increase in drug overdose deaths." Feb 20, 2013. Centers for Disease Control and Prevention. Available: https://www.cdc.gov/media/releases/2013/p0220_drug_overdose_deaths.html [Jan 25, 2017].
89. Bowling, Brian. "Homewood men charged with attempted robbery of pharmaceutical courier." (2016). Available: http://triblive.com/news/adminpage/10639076-74/story [Sep 20, 2016].
90. Freeman, Vernon Jr. "Man wearing surgical mask assaults, robs delivery driver at Chesterfield MARTIN's." (2016). Available: http://wtvr.com/2016/09/08/martins-pharmacy-robbery-and-assault/ [Sep 20, 2016].
91. Armstrong, David. "Pharmacy delivery vans targeted by thieves seeking painkillers." (2015). Available: https://www.statnews.com/2015/12/22/pharmacy-delivery-vans-targeted/ [Sep 20, 2016].
92. "Active Pharmaceutical Ingredient (API) Process Inspection." Food and Drug Administration: Services, Department of Health and Human. 2015.
93. "1988: Thousans die in Halabja gas attack." (n.d.). Available: http://news.bbc.co.uk/onthisday/hi/dates/stories/march/16/newsid_4304000/4304853.stm [Jan 26, 2017].
94. Malsin, Jared. "Assad's Regime Is Still Using Chemical Weapons in Syria." *Time Magazine* (2016). Available: http://time.com/4492670/syria-chemical-weapon-aleppo-assad-regime/ [Jan 26, 2017].
95. "Top intel official confirms ISIS made, used chemical weapons." (2016). Available: http://www.foxnews.com/politics/2016/02/09/top-intel-official-confirms-isis-made-used-chemical-weapons.html [Jan 26, 2017].
96. Hiyama, Hiroshi. "Capture of Japan's most wanted ends hunt for cult that launched Tokyo gas attacks." *The Sydney Morning Herald* (2012). Available: http://www.smh.com.au/world/capture-of-japans-most-wanted-ends-hunt-for-cult-that-launched-tokyo-gas-attacks-20120615-20fa6.html [Jan 26, 2017].
97. Vandiver, John. "Arms Stolen from Weapons Room on US Military Base in Stuttgart." (2016). Available: http://www.military.com/daily-news/2016/07/29/arms-stolen-from-weapons-room-on-us-military-base-in-stuttgart.html [Jan 26, 2017].
98. Rubin, Alissa J. "Thieves Grab Bomb Parts at French Military Base." *The New York Times* (2015). Available: https://www.nytimes.com/2015/07/08/world/europe/bomb-making-parts-stolen-from-french-military-base.html [Jan 26, 2017].
99. Howze, Ray, and Stacey Brachenger. "U.S. Attorney: Fort Campbell soldiers sold stolen Army gear to buyers overseas." (2016). Available: http://www.tennessean.com/story/news/crime/2016/10/06/six-fort-campbell-soldiers-two-civilians-indicted-charges-selling-army-equipment-buyers-11-countries/91666716/ [Jan 27, 2017].
100. "DoD Instruction Number 5210.65, Security Standards for Safeguarding Chemical Agents." Defense, Department of. 2016.
101. "Chemical Munitions Requirements for the Marine Amphibious Force (MAF)." Marine Corps Development and Education Command: Defense, Department of. 1987.
102. "Permissive Links for Nuclear Weapons in NATO." President, Executive Office of the. 1962.

103. "Command and Control Systems for Nuclear Weapons: History and Current Status." SLA-73-0415. Sandia National Laboratories. Energy, Department of. 1973.
104. Cotter, Donald R. "Peacetime Operations: Safety and Security." *Managing Nuclear Operations*. Eds. Carter, Ashton B, John D Steinbruner and Charles A Zraket. Washington, DC: Brookings Institution, 1987. 17-74. Print.
105. Howzit, Sam. "No Lone Zone." 2010. Available: https://www.flickr.com/photos/aloha75/6109624143/ [Oct 11, 2016].
106. "Air Force Instruction 91-104, Nuclear Surety Tamper Control and Detection Programs." Secretary of the Air Force. Defense, Department of. 1993.
107. "Air Force Instruction 91-104, Nuclear Surety Tamper Control and Detection Programs." Secretary of the Air Force. Defense, Department of. 2013.
108. "Civilian Control of Atomic Energy." U.S. Department of Energy. n.d. Available: https://www.osti.gov/opennet/manhattan-project-history/Events/1945-present/civilian_control.htm [Sep 22, 2016].
109. "An Assessment of Current Physical Security Models." RDA-TR-111500-001. R&D Associates. Naval Surface Weapons Center: Defense, Department of. 1979.
110. "Commander's Guide to Nuclear Surety and Explosives Safety." 39th Wing. Defense, Department of. 2011.
111. "Nuclear Safety and Security." *Nuclear Matters Handbook*. Vol.: Office of the Assistant Secretary of Defense for Nuclear, Chemical and Biological Defense Programs, 2011. 61-77. Available.
112. *Preventative and Protective Measures against Insider Threats*: International Atomic Energy Agency (IAEA), 2008. Print.
113. McBride, Jim. "Pantex handoff set for Tuesday." Amarillo Globe-News, 2016. Available: http://amarillo.com/news/latest-news/2014-06-28/pantex-handoff-set-tuesday [Oct 4, 2016].
114. "DOE O 452.2D, Nuclear Explosive Safety." National Nuclear Security Administration: Energy, Department of. 2009.
115. "DOE M 452.2-1A, Nuclear Explosives Safety Manual." National Nuclear Security Administration: Energy, Department of. 2013.
116. Young, Alison. "Congress demands details of secret CDC lab incidents revealed by USA TODAY." *USA TODAY* (2017). Available: http://www.usatoday.com/story/news/2017/01/17/congress-wants-details-of-cdc-lab-accidents/96551636/ [Jan 27, 2017].
117. "Letter to Director Thomas Frieden." Committee on Energy and Commerce: Representatives, United States House of. 2017.
118. Goenka, Himanshu. "Bioterrorism Agents, Deadly Viruses, Bacteria On The Loose? CDC Kept Mishaps With Dangerous Germs Secret, USA Today Finds." (2017). Available: http://www.ibtimes.com/bioterrorism-agents-deadly-viruses-bacteria-loose-cdc-kept-mishaps-dangerous-germs-2470046 [Jan 27, 2017].
119. Moakley, John J. "Pair Charged With Theft Of Trade Secrets From Harvard Medical School." Jun 19, 2002. U.S. Department of Justice. Available: https://www.justice.gov/archive/criminal/cybercrime/press-releases/2002/zhuCharges.htm [Jan 30, 2017].
120. Skerritt, Jen. "Lab didn't tell police 22 vials stolen." (2009). Available: http://www.winnipegfreepress.com/local/lab-didnt-tell-police-22-vials-stolen-45078877.html [Jan 30, 2017].
121. Canada, Public Health Agency of. "National Microbiology Laboratory (NML) Overview." 2015. Available: https://www.nml-lnm.gc.ca/overview-apercu-eng.htm [Mar 27, 2017].
122. "Winnipeg researcher charged with smuggling Ebola material into U.S." *CBC News* (2009). Available: http://www.cbc.ca/news/canada/winnipeg-researcher-charged-with-smuggling-ebola-material-into-u-s-1.774725 [Mar 27, 2017].
123. *Enhancing Personnel Reliability among Individuals with Access to Select Agents*: National Science Advisory Board for Biosecurity (NSABB), 2009. Print.
124. *Department of Defense Biological Safety and Security Program*. Washington, DC: Office of the Undersecretary of Defense For Acquisition, Technology, and Logistics, 2009. Print.
125. *Guidance for Enhancing Personnel Reliability and Strengthening the Culture of Responsibility*: NSABB, 2011. Print.
126. Berger, Kavita M. "What life scientists should know about security threats." *Science* 354.6317 (2016): 1237-39.
127. Council, National Research. *Prudent practices in the laboratory: handling and management of chemical hazards, updated version*. National Academies Press, 2011. Print.
128. Bhattacharjee, Yudhijit. "The danger within." *Science* 323.5919 (2009): 1282-83.
129. Shane, Scott. "Panel on Anthrax Inquiry Finds Case Against Ivins Persuasive." *The New York Times* (2011). Available: http://www.nytimes.com/2011/03/24/us/24anthrax.html [Jan 30, 2017].

130. "Letter Addressed To Senator Patrick J. Leahy Appears To Contain Anthrax." Nov 17, 2001. FBI National Press Office. Available: https://archives.fbi.gov/archives/news/pressrel/press-releases/letter-addressed-to-senator-patrick-j.-leahy-appears-to-contain-anthrax [Jan 30, 2017].
131. "Laboratory Security." Stoney Brook University. n.d. Available: https://ehs.stonybrook.edu/programs/laboratory-safety/laboratory-security [Jan 30, 2017].
132. *TSA Chief Out After Agents Fail 95 Percent of Airport Breach Tests*. Video. Jun 1, 2015.
133. Holmes, James P, Russell L Maxwell, and Ronald W Henderson. "Automated biometric access control system for two-man-rule enforcement." *Nuclear Materials Management Annual Meeting Proceedings*. 1991. Print.

DISTRIBUTION

1	MS9406	Nerayo Teclemariam	8712 (electronic copy)
1	MS9406	Scott Paap	8712 (electronic copy)
1	MS9407	Jarret Lafleur	8718 (electronic copy)
1	MS9045	Dennis Baker	8511 (electronic copy)
1	MS9031	Patricia Koning	8524 (electronic copy)
1	MS9107	John Paulson	0021 (electronic copy)
1	MS9108	Rich Moore	8771-1 (electronic copy)
1	MS9960	Technical Library	8744 (electronic copy)


Sandia National Laboratories