Organizing Risk Management Programs

Or, What I learned from the Aviation Industry and the US Secret Service

TRANSVASIVE

Transparent and Pervasive Security

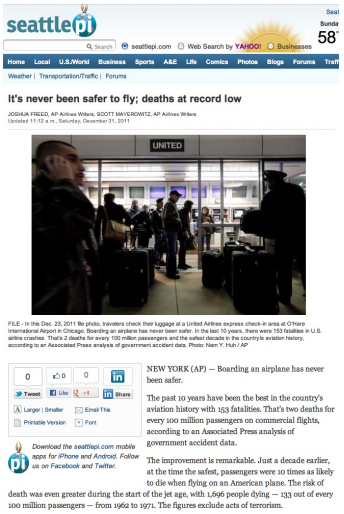
Good Afternoon, Introduction.

Aviation Industry: Safety
US Secret Service: Protection

SUCCESSFUL RISK MANAGEMENT

When I went looking for highly effective risk management programs, I found a couple of interesting examples that were different in interesting ways: the Aviation Safety Industry and the US Secret Service. **Both have stories of innovation over the past 10 years that improved how they managed risk.**

Safety: Aviation Industry



seattlepi

It's never been safer to fly; deaths at record low

JOSHUA FREED, AP Airlines Writers, SCOTT MAYEROWITZ, AP Airlines Writers

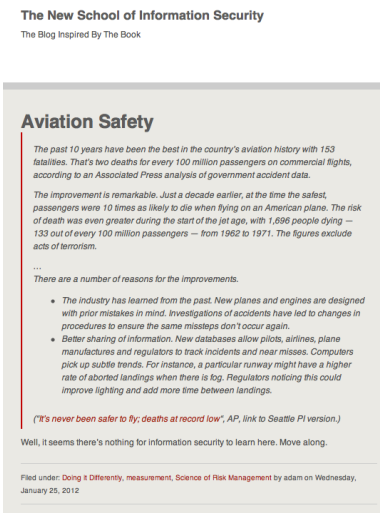
Updated 11:12 a.m., Saturday, December 31, 2011

FILE - In this Dec. 23, 2011 file photo, travelers check their luggage at a United Airlines express check-in area at O'Hare International Airport in Chicago. Boarding an airplane has never been safer. In the last 10 years, there were 153 fatalities in U.S. airline crashes. That's 2 deaths for every 100 million passengers and the safest decade in the country's aviation history, according to an Associated Press analysis of government accident data. Photo: Nam Y. Huh / AP

NEW YORK (AP) — Boarding an airplane has never been safer.

The past 10 years have been the best in the country's aviation history with 153 fatalities. That's two deaths for every 100 million passengers on commercial flights, according to an Associated Press analysis of government accident data.

The improvement is remarkable. Just a decade earlier, at the time the safest, passengers were 10 times as likely to die when flying on an American plane. The risk of death was even greater during the start of the jet age, with 1,696 people dying — 133 out of every 100 million passengers — from 1962 to 1971. The figures exclude acts of terrorism.



The New School of Information Security

The Blog Inspired By The Book

Aviation Safety

The past 10 years have been the best in the country's aviation history with 153 fatalities. That's two deaths for every 100 million passengers on commercial flights, according to an Associated Press analysis of government accident data.

The improvement is remarkable. Just a decade earlier, at the time the safest, passengers were 10 times as likely to die when flying on an American plane. The risk of death was even greater during the start of the jet age, with 1,696 people dying — 133 out of every 100 million passengers — from 1962 to 1971. The figures exclude acts of terrorism.

...

There are a number of reasons for the improvements.

- *The industry has learned from the past. New planes and engines are designed with prior mistakes in mind. Investigations of accidents have led to changes in procedures to ensure the same missteps don't occur again.*
- *Better sharing of information. New databases allow pilots, airlines, plane manufactures and regulators to track incidents and near misses. Computers pick up subtle trends. For instance, a particular runway might have a higher rate of aborted landings when there is fog. Regulators noticing this could improve lighting and add more time between landings.*

("It's never been safer to fly; deaths at record low", AP, link to Seattle PI version.)

Well, it seems there's nothing for information security to learn here. Move along.

Filed under: Doing It Differently, measurement, Science of Risk Management by adam on Wednesday, January 25, 2012

The aviation industry has a safety culture that has developed over the past 75+ years. Over that time, advances in safety, including checklists, safety controls, CRM (Crew Resource Management), and LOSA (Line Operations Safety Audits) **have made air travel extraordinarily safe**.

http://www.seattlepi.com/news/article/It-s-never-been-safer-to-fly-deaths-at-record-low-2434524.php by way of http://newschoolsecurity.com/2012/01/aviation-safety/

Safety: Aviation Industry

Boeing Model 299: Checklists

Decisions on implementing safety controls

Tenerife: Crew Resource Management

Line Operations Safety Audits

The October 1935 crash of the Model 299 aka B-17 (the takeoff sequence exceeded the limits of human memory) led to a major advance in aviation safety that is now an essential component of every flight, the checklist.

http://www.atchistory.org/History/checklst.htm
Photo: http://www.nationalmuseum.af.mil/shared/media/photodb/photos/060706-F-1234S-002.jpg by way of http://en.wikipedia.org/wiki/Boeing_B-17_Flying_Fortress_variants

Safety: Aviation Industry

Boeing Model 299: Checklists

Decisions on implementing safety controls

Tenerife: Crew Resource Management

Line Operations Safety Audits

Aviation Safety puts a price on human life. The valuation is set to be the settlement amount for a typical wrongful death lawsuit against an airline following a fatal plane crash. The industry uses this measure of impact, along with estimates of likelihood of fatalities occurring based on prior knowledge to decide whether or not to implement a given safety measure. This makes risk management a (relatively) easy decision: **if the cost to reduce the likelihood of a given incident is less than the risk reduction, the safety measure is implemented**. (Of course, the reality is more complicated)

Photo: http://en.wikipedia.org/wiki/File:Euromoenterogsedler.jpg

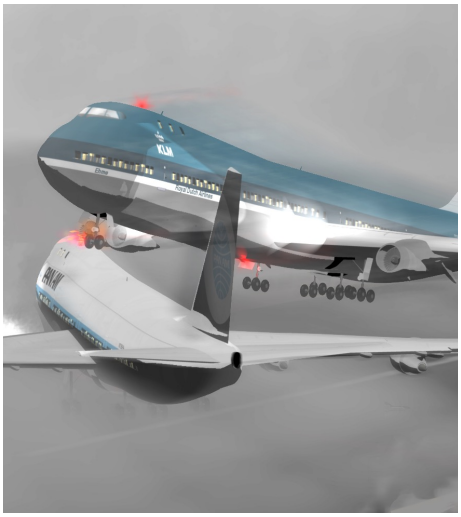
Safety: Aviation Industry

Boeing Model 299: Checklists

Decisions on implementing safety controls

Tenerife: Crew Resource Management

Line Operations Safety Audits



Tenerife = **worst accident in history, 583 fatalities, March 27, 1977**. Captain Jacob van Zanten, KLM's most senior pilot, started takeoff while a Pan Am plane was still on the runway. The tragic accident led to an important improvement in safety, Crew Resource Management.

CRM encourages a **respectful questioning of authority**, but also improved communication, decision making, and most importantly, allows errors to be trapped and managed to an inconsequential outcome. ***(Without hurting people's feelings)***

http://en.wikipedia.org/wiki/Tenerife_disaster
http://en.wikipedia.org/wiki/Crew_resource_management
Photo: http://en.wikipedia.org/wiki/File:Tenerife747s.png

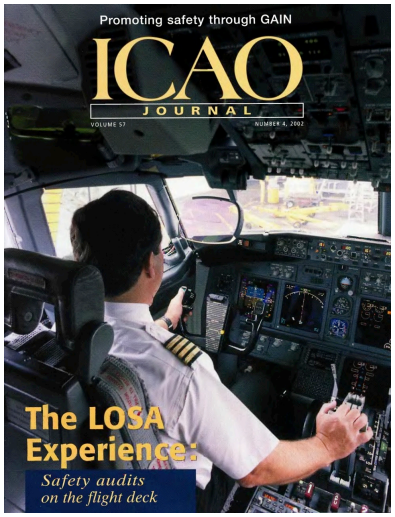
Safety: Aviation Industry

Boeing Model 299: Checklists

Decisions on implementing safety controls

Tenerife: Crew Resource Management

Line Operations Safety Audits



LOSA is an innovation that placed trained observers in the cockpit during normal flights to observe the behaviors of the crew, and to collect and report on errors and the consequences of the errors anonymously with the goal of improving safety. LOSA has been in use over the past ~10 years.

LOSA accepts and acknowledges that human error is inevitable, and gives crews permission to be observed as well as talk openly with the LOSA observer about errors, without fear of punishment. LOSA's proven effectiveness has led to its adoption outside the cockpit, in both maintenance and ramp operations.

A Culture of Safety: Aviation safety has evolved over the years to prove remarkably effective at managing environmental threats, but even more so at managing the constant threat of human error. From the origin of checklists, through CRM and now LOSA, acknowledging human limits, **including the impact of emotion on safety**, and creating methodologies for managing those limits is a hallmark of the aviation safety industry.

http://homepage.psy.utexas.edu/homepage/group/helmreichlab/aviation/LOSA/LOSA.html
http://homepage.psy.utexas.edu/homepage/group/helmreichlab/publications/249.pdf
http://www.faa.gov/library/online_libraries/aerospace_medicine/sd/media/Helmreic

.pdf

Protection: US Secret Service

For over 100 years, (following the assassination of President William McKinley in 1901) the Secret Service has been charged with protection duties, to prevent violent attacks against the president, other national leaders and foreign dignitaries.

http://en.wikipedia.org/wiki/United_States_Secret_Service
Photo: http://en.wikipedia.org/wiki/File:Reagan_assassination_attempt_4_crop.jpg

Protection: US Secret Service

Exceptional Case Study Project

National Threat Assessment Center

Safe School Initiative (NTAC)

Insider Threat Study (NTAC/CERT)

Completed in 1998, the Exceptional Case Study Project, reviewing "the thinking and behavior of all 83 persons who planned or executed attacks against public figures in the United States from 1949 to 1996." Their study exposed both myths as well as commonalities in the attacks and attempted attacks.

Myth: Assassins fit a "profile". They do not.
However, the study also discovered that all would-be assassins have a common behavior profile:

- Exhibiting organized thinking and behaviors
- Seeing the attacks as a means to a goal, **especially as a violent response to unbearable stress**

In response to these findings, the Secret Service created the National Threat Assessment Center (NTAC).

http://www.secretservice.gov/ntac.shtml
Photo: http://en.wikipedia.org/wiki/File:Jared_Loughner_USMS.jpg

Protection: US Secret Service

Exceptional Case Study Project

National Threat Assessment Center

Safe School Initiative (NTAC)

Insider Threat Study (NTAC/CERT)

The Threat Assessment process developed by the NTAC has three main components: Identification, Assessment, and Case management.

Identification: Identify potential threats.
Assessment: Evaluate if the subject poses a threat. (Interview, Investigation)
Case Management: "Manage" the threat.

The threat assessment approach is a modern innovation that blurs the lines between social work and law enforcement. Instead of investigating and punishing perpetrators of crimes, threat assessment seeks to intervene in a potential criminal's life and divert them from the escalation path to violent attacks. (help)

http://www.secretservice.gov/ntac.shtml
Photo: http://en.wikipedia.org/wiki/File:US-SecretService-StarLogo.svg

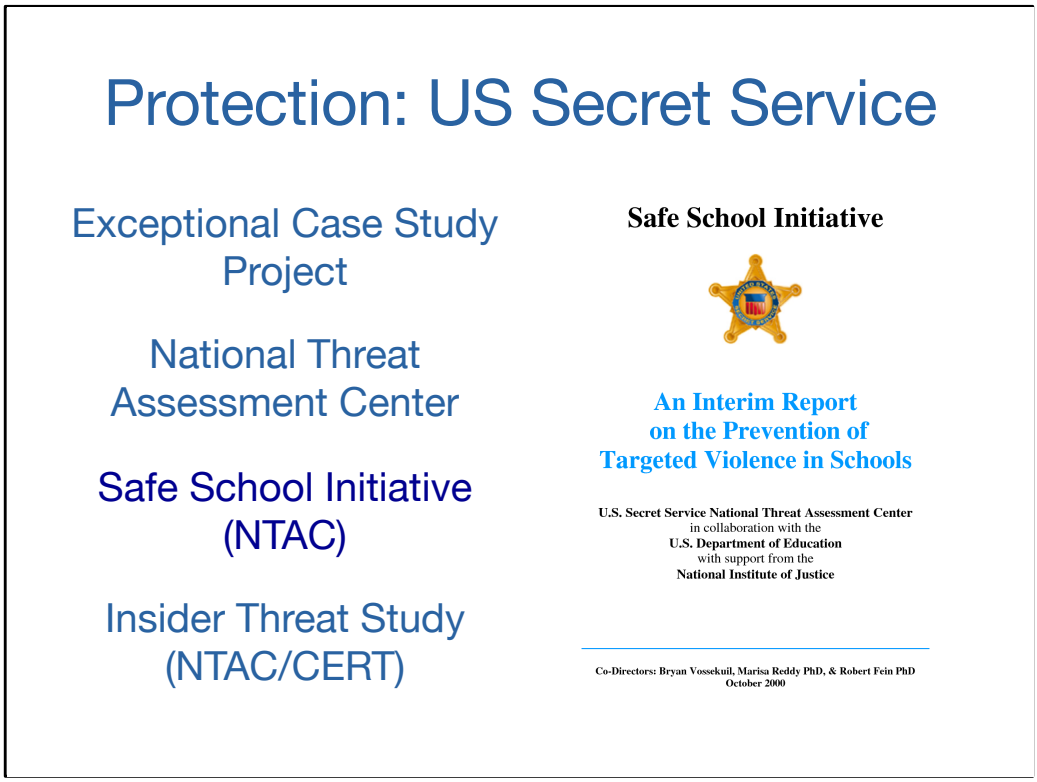
Protection: US Secret Service

Exceptional Case Study Project

National Threat Assessment Center

Safe School Initiative (NTAC)

Insider Threat Study (NTAC/CERT)



NTAC's research includes studying school violence, the Safe School Initiative (SSI) and found similar results, suggesting the usefulness of threat assessment beyond protective services.

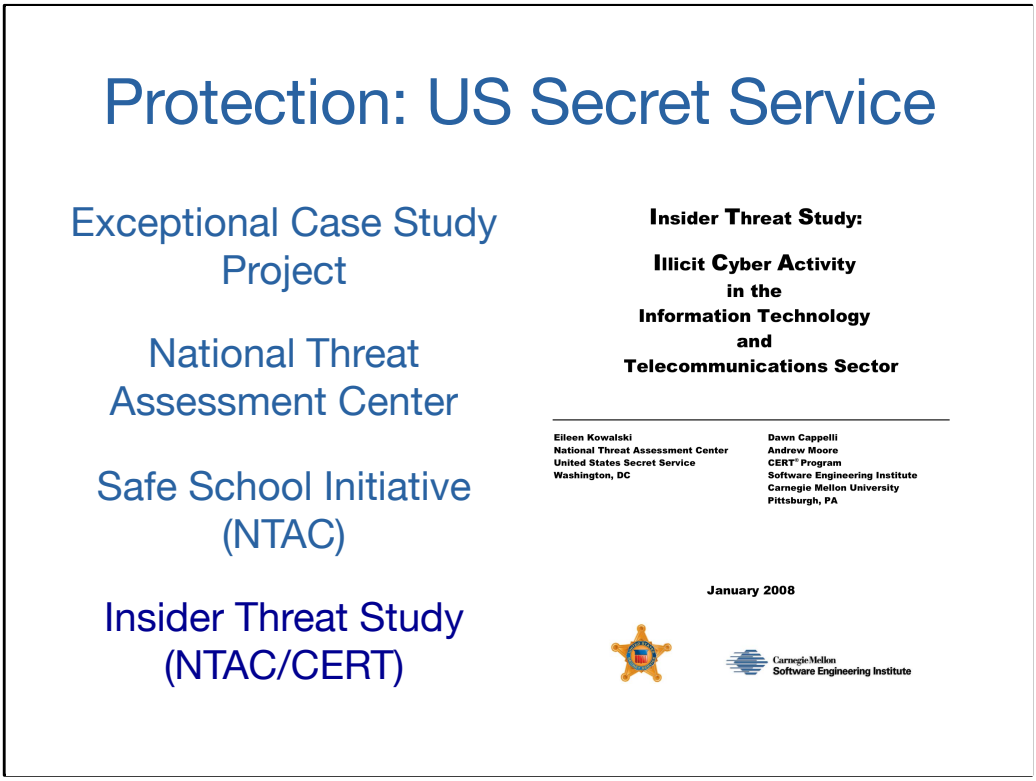
Protection: US Secret Service

Exceptional Case Study Project

National Threat Assessment Center

Safe School Initiative (NTAC)

Insider Threat Study (NTAC/CERT)



Insider Threat Study:

Illicit Cyber Activity in the Information Technology and Telecommunications Sector

Eileen Kowalski
National Threat Assessment Center
United States Secret Service
Washington, DC

Dawn Cappelli
Andrew Moore
CERT® Program
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA

January 2008

Carnegie Mellon Software Engineering Institute

NTAC/CERT study again found that while malicious insiders did not share a common profile, they did exhibit common behaviors.

- Planned the attack
- Had job-related issues (motive)
- Did not consider the severity of the consequences

The common theme across all NTAC's research is that while **profiling the background of potential attackers doesn't work, profiling their behaviors does**. Distinguishing a potential attacker from a harmless innocent by observing their behavior patterns (while ignoring their demographic characteristics) is potentially a general method for identifying malicious behavior.

Tale of Two Industries

Safety (Aviation Industry)

- Robust data set
- Statistics are useful
- Incidents are accidents
- Wait until an incident occurs, then react
- Data-driven
- Costs of incidents are measurable
- Threats are common and frequently encountered
- Threats are environmental or human errors
- Threats don't adapt to new safety controls
- Innovations have come from understanding and changing our own behaviors
- Decision making aided by tools like checklists, Crew Resource Management
- Risk Analysts biased to see everyone as only committing inadvertent errors
- Boring

Protection (US Secret Service)

- Limited data
- Statistics have limited usefulness
- Incidents are deliberate
- Find, manage threats before they can act
- Intelligence-driven
- Costs of incidents are difficult to measure
- Threats are uncommon and infrequently encountered
- Threats are people with malicious intent
- Threats adapt to new security controls
- Innovations have come from understanding and managing threat behaviors
- Decision making reliant on investigation, professional judgment
- Risk Analysts biased to see everyone as a potential threat
- Sexy

The patterns of a successful safety program are distinctly different from the patterns of a successful protection program. While safety, embodied by the Aviation Industry, has an inward focus, Protection, embodied by the Secret Service, has an outward focus.

Notably, neither discipline spends much time on vulnerability management. Some quick searching with Google reveals that the idea of vulnerability management seems unique to the Information Security profession. Also notably, both leverage information sharing to improve risk management.

Information Safety
Information Protection

ORGANIZATION OF RISK MANAGEMENT

What does this mean for how we organize an information risk management program?

I propose that we should split information risk management into Information Safety and Information Protection functions, **employing Safety where we find conditions like in the Aviation Industry, and Protection where we find conditions like in the Secret Service.**

Fraud is an interesting case, and has elements that are best addressed by both Safety and Protection. In its steady state, fraud events happen frequently and threats are slow to adapt, however, **new innovations in fraud happen infrequently and when they do, cause unpredictable results.**

By splitting risk management into Safety and Protection, we can leverage the distinct strengths of each discipline to specific risk management problems. Ideally, these would be two separate teams, but that only becomes practical in very large organizations; in smaller orgs, recognizing them as separate disciplines is a good substitute. As safety appears to require less manpower, resources, has more measurable usefulness, and doesn't require law enforcement authority, establishing a safety function first is recommended for all organizations. This is reflected in the fact that the Safety examples are generally representative of the actual priorities of most security organizations. Protection should normally be relegated to external organizations, either for-hire private security firms or law enforcement. For those that are large enough to staff a protection function, protection will likely be small in comparison to the safety team.

I was fortunate enough to sit next to Donn Parker at a risk management roundtable at RSA this year. Donn, who has been working in information security longer than I've been alive and not a believer in risk management, related a couple of personal experiences that I will try to accurately represent. First, he described a fraud

department that presented a chart that should a marked increase in fraud. The fraud team knew exactly what had happened; it was when the local mob had started a campaign against the company. Second, he described a case (I don't recall the details) where a single incident led to a significant loss, making a risk profile like the fraud team had impossible. In his 2006 article, *Making the Case for Replacing Risk-Based Security,* Donn puts forth a similar argument: there are two types of problems information security: ongoing attacks that are virtual certainties, like viruses, and rare, unpredictable incidents. I agree with his observations, but disagree (somewhat) with his conclusion: use a time-tested due diligence approach – do what we have always done. To me, these two distinct flavors of information security describe the two types of risk management: Safety and Protection. **I do believe by dividing risk management into two we can improve upon due diligence. And, like the ESCP, I believe we will discover some of our beliefs are myths while others are good risk management.**

Information Safety for Security Awareness & Education

- DON'T teach people how to assess risk
- DO teach people how to be safe

- DON'T teach threat assessment skills
- DO teach CRM skills

- DON'T worry about the bad guys
- DO worry about ourselves

Photo: http://en.wikipedia.org/wiki/File:Pogo_-_Earth_Day_1971_poster.jpg

Questions? Also, please feel free to stop up and grab one of my business cards.