SECURITY EXECUTIVE COUNCIL
A research and advisory firm

Demonstrating Value > Operational Excellence >

Case Study: Risk Management and Security Metrics at Boeing

Created by David Niehaus,[1] University of South Carolina

Boeing Corporation is one of world's major aerospace and information technology firms. Its products include commercial aircraft, military aircraft, satellites, and rocket launch systems, as well as products and services supporting information and network systems. At the end of 2011, Boeing had over 171,000 employees, located in 70 countries at more than 400 different sites. The company is organized in five segments.

(1) The Commercial Airplane segment develops, produces, and provides support services for the commercial airline industry. Products and services include the 747 and 767 airplanes, aircraft modifications, and training. Major competitors include Airbus, Embraer and Bombardier.

(2) The Military Aircraft segment conducts research on, develops, produces, and supports a wide range of defense aircraft. Products include the Apache and Chinook helicopters, the F-15 and F-22 fighter jets, tankers for refueling in the air, and a variety of munitions.

(3) The Network & Space Systems segment conducts research on, develops, and produces products and services to help customers more effectively and efficiently gather, analyze, and communicate information. Products include the Combat Survivor Evader Locator (CSEL) and the Enhanced Medium Altitude Reconnaissance and Surveillance System (EMARSS).

[1] This project was made possible by the financial support and coordination efforts of the Security Executive Council. The author appreciates the time, encouragement, and feedback from George Campbell, Francis D'Addario, Bob Hayes, and Kathleen Kotwica. In addition, the project could not have been undertaken without the openness and participation of Dave Komendat, Vice President and Chief Security Officer of the Boeing Corporation, and the administrative support of several people on his staff, especially Cindy Wall.

(4) The Global Services and Support segment provides maintenance, training, upgrades, and logistics support for military products produced by the company. In 2011, 76 percent of the revenues from the Military Aircraft, Network and Space Systems, and Global Services & Support segments came from the U.S. Department of Defense. The major competitors for these three segments include Northrop Grumman, Raytheon, General Dynamics, and BAE Systems.

(5) The Boeing Capital Corporation segment provides financing solutions (e.g., operating leases, notes, etc.) for the company's customers.

Exhibit 1 summarizes the revenues and earnings generated by each of the business segments in 2011. More than half of Boeing's revenue and earnings were generated by the Commercial Airplane segment.

Exhibit 1. Boeing's 2011 Revenues & Earnings from its Business Segments

Segment	Revenue*	% of Total	Earnings*	Operating Margin
Commercial Airplanes	36,171	52.7%	3,495	9.7%
Military Aircraft	14,947	21.8%	1,526	10.2%
Network & Space Systems	8,673	12.6%	690	8.0%
Globas Services & Support	8,356	12.2%	942	11.3%
Capital Corporation	532	0.8%	125	23.5%
Total	68,679		6,778	
* in millions of dollars				

BOEING'S SECURITY & FIRE PREVENTION GROUP

The following description of the Security & Fire Prevention (S&FP) group's mission and scope of responsibilities comes from a document that was released by Boeing in May 2012. The Boeing Security & Fire Protection organization is responsible for providing risk management services, governance standards and site-based security and fire protection services to protect Boeing's people, property and information and support business resiliency.

Responsible for meeting national security standards related to defense systems and technology export control that helps safeguard sensitive, proprietary and classified information, Security & Fire Protection also maintains and monitors building and classified network security.

The organization has enterprise wide responsibility to ensure that appropriate emergency preparedness plans are in place to address safety, evacuation and suspension of operations in the event of a fire, natural disaster, hazardous materials release, bomb threat or any other type of emergency. It also has the Business Continuity group, whose primary objective is to help the business units develop plans that enable risk mitigation and recovery of critical processes, operations, assets and infrastructure in the event of a work disruption.

Boeing Security also oversees the company-wide program to reduce the risk of violence in the workplace.

Boeing Security helps determine and enforce export and import requirements, including interpretation of appropriate laws and regulations, and oversees security clearances required in many areas within the company for employees, visitors and contractors. The organization also has responsibility for employment and contractor background screening as well as handling and ensuring all credentialing requirements for employees and visitors.

Two organizations within Boeing Security focus on ensuring domestic and international security. The Domestic Security Activity (DSA) and International Security Activity (ISA) organizations enable Boeing business partners to support event security at special events and air shows, protect assets, respond to crises and incidents, mitigate risk and remain compliant within the U.S. and abroad. Working with partners across the company and with external organizations, DSA has established processes to deal with espionage and terrorism threats to Boeing; the ISA specializes in international travel security at numerous locations around the world.

In addition to focusing on domestic and international security, Security & Fire Protection plays a leadership role in crisis management. In the event of a natural disaster, political turmoil, terrorism or an operational shut down, Boeing Security, together with other enterprise wide organizations, joins together to establish evacuation, shut down, continuity and resumption plans. The function of this Crisis Management Team is to rapidly mitigate a crisis, minimize danger to Boeing personnel and prevent the loss of company assets.

The Security & Fire Protection organization oversees the company Fire Department, which is one of the largest and best-trained private, industrial fire prevention agencies in the country. Additionally, a team of certified hazard materials experts respond to hazmat incidents, and Fire Protection Engineering – the technical arm of Boeing's fire prevention and inspection program – provides fire hazard analysis and fire protection design support and review.

The organization’s Uniformed Security Officer Team is comprised of more than 1,200 experienced and knowledgeable Boeing employees and contract security officers who secure Boeing facilities across the enterprise around the clock, 365 days a year. Within

Boeing Security, the Explosive Detection Dog program helps to provide a safe work environment for Boeing employees, contractors and visitors. K-9 teams are deployed at various key locations throughout the U.S.

BACKGROUND ON RISK MANAGEMENT METRICS

Metrics are used in all areas of business to inform decision making, influence behavior, and evaluate performance. When developing metrics, it is important that they be linked to organizational objectives. For example, if one organizational objective is to increase shareholder value, then metrics should inform managers about how decisions would affect value. Similarly, metrics that help managers evaluate how past decisions affected value would be applicable as well.

The risk management process involves (1) the identification of risks, (2) an assessment of the probability distribution of outcomes (e.g., frequency and severity of losses), and (3) the evaluation of alternative methods of dealing with the risk, i.e., whether to retain the risk or to alter the organization's exposure through some combination of avoidance, mitigation, or transfer. Risk management decisions almost always involve tradeoffs. For example, avoidance of a particular risky activity implies that the potential benefits of that activity will not be realized, and mitigation and transfer almost always involve some costs. An organization's objectives provide the guidance for thinking about these tradeoffs.

Most organizations have broad overarching goals (e.g., increasing value), which in turn lead to more specific narrower goals for individual units within the organization. These unit goals are typically tied to the specific activities of the group. Correspondingly, the metrics used in a particular unit should correlate to the unit's specific goals and activities. Boeing's S&FP group provides a good example of this. The unit is specifically tasked with protecting human, physical, and information assets from potential losses and with enabling the other business units within the organization to perform. Therefore, the metrics used by Boeing should provide information that will help managers achieve these tasks. It is often recommended that metrics be SMART[2], i.e., they should be

- Specific - they target the area one is measuring.
- Measurable - one is able to collect data which is accurate and complete
- Actionable - they are easy to understand and help one decide when to take action.
- Relevant – they are measuring something that is important to organization's goals
- Timely – data is readily available and accessible

[2] See J. W. Wesner et al, Winning with Quality, Addison-Wesley, Reading, MA, 1995.

It is also useful when designing metrics for security and risk management purposes to have metrics that are tied to the risk management process. That is, metrics should help identify risk exposures for further consideration, or help assess the likelihood and severity of potential losses, or provide information that helps managers compare the costs and benefits of retention, avoidance, mitigation, and transfer.

The risk exposures that are of concern to security and risk professionals often evolve over time. For example, information about the likelihood of property damage from hurricanes will evolve, as new information about storms in the Atlantic Ocean is uncovered. It is therefore useful when designing risk assessment metrics to distinguish leading indicators (or metrics) and lagging indicators.[3] Leading indicators provide information about the likelihood and or severity of potential events prior to their occurrence. Metrics that track the wind speed and location of tropical storms would be examples of leading indicators of property damage to a facility on the gulf coast. Ideally, leading indicators provide actionable information to mitigate potential damage.

Lagging indicators provide information about what has already happened. Lagging indicators often involve count data, e.g., the number of injuries suffered or the value of property damaged incurred. While these data can provide useful information about potential future events, they do not necessarily incorporate the context of a specific event. For this reason, it is often useful to conduct a detailed analysis of an incident or what is sometimes called an incident post-mortem. These detailed analyses can lead to actionable conclusions about what can be done better in the future.

THE REVIEW AND EVALUATION OF METRICS AT BOEING

In 2009, Dave Komendat, the head of S&FP, and his top management team determined that the S&FP group needed to improve its ability to measure and communicate how the group was providing value to the entire Boeing organization. Dave believed that there were numerous ways that his group created value, and he also believed that there were other ways the S&FP group could create additional value for the organization if given more resources. For example, he believed that the S&FP group could, in a cost-effective way, provide

- Greater protection of assets
- Reduced likelihood of interruptions to revenue generating activities
- Greater awareness and engagement of employees in securing assets
- Increased market penetration attributable to security measures
- Faster recovery time following interruptions of critical processes
- Reduced cost of insurance with comparable or more coverage

[3] See Campbell, George, Measures and Metrics in Corporate Security: Communicating Business Value, Security Executive Council, 2007.

Although the security group collected lots of data, Dave believed that there was a need to develop new metrics that demonstrated the value created by the security group to top managers.

Dave contracted with the Security Executive Council (hereafter the Council) to conduct a review of the group's use of metrics. The Council called upon George Campbell and Francis D'Addario to assist Dave's team.[4] For their review, George and Francis interviewed a number of people at Boeing and read numerous reports. Their overall conclusions were that Boeing's data collection and management could be improved. More specifically, data collection and management could be more focused on providing actionable information, and data management resources could be allocated more efficiently. In addition, they found that Boeing had numerous opportunities to develop a set of metrics that would help the group showcase the value, quality, and cost efficiencies that were being provided.

Regarding data management, George and Francis found that the security group was spending significant effort in collecting and warehousing data, but that much of the collected data was too focused on counting inputs (e.g., number of first responder calls) or counting the number of incidents that occurred (e.g., number of false alarms), and not sufficiently focused on information that could be used to identify, assess, or evaluate risks. For example, too little data on injury and damage costs were being collected; these data are necessary for assessing risk and making risk mitigation decisions. As a consequence, some of the data being collected was not useful for assessing the value provided by the security group.

George and Francis also found that the useful information that was being collected was not assembled in a way that other groups in the broader organization could learn from the input. As a consequence, a comprehensive, enterprise-wide perspective on various risks was not possible, and the development of more efficient risk management practices was hindered. Instead, information remained dispersed within silos. George and Francis recommended that resources be reallocated to promote a more centralized administration and analysis of data, which could then be shared across groups.[5]

[4] George was the former chief security officer (CSO) of Fidelity Investments, the largest mutual fund company in the U.S. In addition, George has authored a book entitled "Measures and Metrics in Corporate Security: Communicating Business Value," which is published by the Council. Francis previously led security operations at Starbucks Coffee and is the co-developer of RED, an enterprise risk event reporting and analytics tool.

[5] IT asset security provides an extreme example. Organizationally, responsibility for IT asset security rested in a different group than S&FP, which resulted in minimal sharing of relevant information. One positive outcome of the review was greater collaboration between the IT risk management group and the S&FP.

Regarding metrics that could be developed, George and Francis had numerous recommendations. The recommendations can be classified in the following categories: (1) Compliance Metrics, (2) Key Threat Metrics, and (3) Value Metrics.

Compliance Metrics. Boeing must comply with numerous regulations and statutory provisions to remain viable, and much of the data being collected was used to demonstrate compliance. George and Francis believed that Boeing could use the data in more productive ways, in addition to demonstrating compliance. For example, OSHA mandates that employers are required to provide a "safe" work environment. While not required by OSHA, Boeing introduced a Background Screening Program to help demonstrate compliance. The background screening process improves workplace safety by proactively reducing the chance that individuals prone to criminal behavior will be permitted onto or near Boeing property. The program also reduces the probability that Boeing property and information will be damaged or lost.

Key Threat Metrics. Because of its business, size, and brand recognition, Boeing is a potential target for a variety of adversaries. The efficient allocation of resources to mitigate potential threats is enhanced by intelligence gathering and frequent diagnosis of the likelihood of various events. Most of the processes and procedures for collecting such information are proprietary and cannot be discussed in this document. Suffice it to say that Boeing has metrics that provide timely information on a variety of threats.

Value Metrics. One of the primary objectives of the review was to enhance the S&FP group's capability in providing value to Boeing. There are a number of ways that this can be done, including

- Reducing insurance costs due to cost effective mitigation efforts
- Reducing security costs while maintaining or enhancing security levels
- Identifying new risk exposures and mitigating them in a cost-effective manner
- Reducing recovery time for business processes following events
- Improving safety (reduced fatalities and/or injuries) in a cost effective manner

An interesting example of data that can be used to demonstrate value is the number of laptops that uniformed personnel secured. These are laptops that were either stolen or left unsecured, and then found by uniformed personnel. Exhibit 2 indicates the number of laptops secured from 2005 to 2010. This is the type of count data that was being collected by Boeing.

Exhibit 2. Number of Laptops Secured

Year:	2005	2006	2007	2008	2009	2010
Laptops secured	140	150	510	660	390	280

The question is “did this activity add value?” Prior to the analysis by George and Francis, Boeing simply counted the incidents that occurred. They did not push the use of metrics further to shed light on the important question of whether value was being added by the group.

To address this issue, George and Francis found a study conducted by the Intel Corporation and Ponemon Institute, which surveyed 138 companies and found that the average cost to these companies of a lost laptop was $49,246 in 2009. The components of these costs are listed in Exhibit 3.

Exhibit 3. Cost Associated with a Lost Laptop

Replacement cost	$1,562
Detection cost	262
Forensics & investigation costs	814
Data breach cost	39,297
Intellectual property loss	5,871
Lost productivity cost	243
Other legal/regulatory cost	1,117
Total averatge cost	$49,246

Even if the benefit of each laptop secured equaled half of the estimated cost of a lost laptop from the Intel study, then the benefit to Boeing from securing 280 laptops in 2010 was $6,894,440 (280 X $49,246/2). This activity alone would cover the annual cost of a number of uniformed personnel, suggesting that the activity generated value for Boeing.

BACKGROUND AND DATA ON WORKPLACE VIOLENCE

Workplace violence generally refers to nonfatal violent crimes against persons either at work or on duty. These incidents include rape/sexual assault, robbery, and aggravated and simple assault. In 2009, there were over 570,000 such incidents in the U.S., which accounted for roughly 24 percent of nonfatal violence against employed persons age 16 or older. The rate of nonfatal violent crime has declined over the past two decades, as the number of incidents per 1,000 workers has dropped from 16 in 1994 to about 4 in 2009. In addition, the decline in workplace violence during this period has been greater than the decline in non-workplace violence[6].

[6] Harrell, Erica (2011), Workplace Violence, 1993-2009, Us Department of Justice, Bureau of Justice Statistics.

Information on workplace homicides are typically separated from other workplace violence incidents. The number of homicides in the workplace in 2009 equaled 521. Workplace homicides have also declined over the past decade, as the number of workplace homicides in 1993 was over 1,000.[7]

It is useful to categorize workplace violence incidents by the type of perpetrator: (1) acts by criminals with no connection to the workplace who enter to commit another crime such as robbery, (2) acts by people to whom the organization provides services, e.g., customers, (3) acts by current or former employees against other employees, and (4) acts by someone with a personal relationship with an employee, such as a spouse.

The vast majority (almost 80 percent) of workplace homicides fall into category (1) and typically occur in retail companies with cash on hand, such as gas stations. Category (2) cases occur most frequently in the healthcare industry. Category (3) and (4) incidents represent situations in which specific employees are targeted, and therefore warning signs often are present, which in turn implies that prevention programs can have an impact.[8]

Although difficult to quantify precisely, the potential costs associated with workplace violence can be high. The costs include damages and legal fees from lawsuits, medical costs, lost productivity for the victim and coworkers, higher turnover and therefore greater employee training cost, low morale, higher wages to compensate employees for increased workplace violence risk, post-event counseling services, additional security measures, repair and clean-up costs, and lost managerial time dealing with incidents.

MITIGATING WORKPLACE VIOLENCE[9]

Boeing, like most major corporations, has workplace violence prevention programs. These programs often include pre-employment screening (e.g., background checks), identification of potential threats (behavior or risk factors that sometimes precede workplace violence), policies for dealing with potential threats (e.g., when to intervene), and procedures and training for responding to incidents.

While workplace violence is difficult to predict and there is no one behavior or indicator by itself that predicts violence, there are behaviors and situations that often precede incidents. For example, personality conflicts between workers, disciplinary action against a worker, and drug or alcohol use on the job are sometimes precursors of workplace violence. Other risk factors or indicators include belligerence, specific threats, outbursts of anger, and fascination with weapons or violence. The overall workplace

[7] ibid
[8] Rugala, et al., ed. *Workplace Violence, Issues in Response*, Critical Incident Response Group, National Center for the Analysis of Violent Crime, FBI Academy, Quantico, Virginia.
[9] Most of the material from this section is found in Workplace Violence: Issues in Response (no date), Critical Incident Response Group, National Center for the Analysis of Violent Crime, FBI Academy, Quantico, Virginia.

environment also can increase the likelihood of violence. For example, understaffing, layoffs, labor disputes, poor management, and high injury rates have been associated with workplace violence. Note, however, that the vast majority of cases in which one or more of these indicators exist will not lead to workplace violence.

Often the potential indicators of violence surface only if employees report them. As a consequence, a workplace culture that encourages employees to report violent and threatening behavior is critical. In addition, managers need to respond to reports of threats; otherwise, it will discourage future reporting. Training employees to identify threats and warning signs can also help reduce violence. Figure 1 provides an overview of the many facets of a comprehensive workplace violence mitigation program.

Boeing has put in place a workplace violence prevention program that encourages employees to report potential threats and designates responsibility for investigating and responding to potential threats.

This article was originally published in 2014 in the Journal of Applied Risk Management and Insurance

Visit the Security Executive Council website for other resources in the Demonstrating Value: Operational Excellence series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more.

Contact us at: contact@secleader.com

Website here: https://www.securityexecutivecouncil.com/

