CHAPTER

9

SECURITY-RISK ANALYSIS[1]

Farrokh Alemi and Jennifer Sinkule

These days, there is a palpable frustration with risk analysis and vulnerability assessments because critics believe they have misdirected security and recovery efforts. Some think these tools are misinforming people and causing an epidemic of fear (Siegel 2005). Organizations may misunderstand small probabilities of rare events and may seek remedies that cause more harm than the original threat would have (Gray and Ropeik 2002).

Other critics point out that the real problem is not miscommunication about the risk but faulty analysis leading to wrong priorities (Siegel 2005). Organizations may protect against long lists of security threats that are not likely to happen and fail to safeguard against prevalent risks. For example, such reviews may put an anthrax terrorism attack (Leask, Delpech, and McAnulty 2003) at a higher risk level than a hurricane as devastating as Katrina; obviously, the hurricane has more devastating impact. People using risk analysis need to be more accurate in the way they set priorities for action and ranks potential threats.

Let's start with a few obvious principles and assumptions. Risk analysis does not help when the outcome is a recommendation that all security steps are equally important and should be pursued. To be helpful, risk analysis must help organizations set priorities. To set priorities, there must be a process that could establish that the risk of one event is higher than another. To help groups understand differential risks, risk analysis must be based an objective, defensible fact; relying on consensus is not enough unless one can show that the consensus is based on actual events. This chapter shows how the accuracy of risk analysis could be improved by shifting away from consensus and comprehensive vulnerability assessments to more a focused, probabilistic, and objective analysis.

There are three possible objections to probabilistic and focused (not comprehensive) security analysis. The first is that terrorism and major catastrophic events are rare, and therefore it is not possible to measure their frequency (Kollar et al. 2002). Second, the approach is not practical; a probabilistic risk assessment is too time consuming and cumbersome. Finally, the approach should not be done because objective risk

This book has a companion web site that features narrated presentations, animated examples, PowerPoint slides, online tools, web links, additional readings, and examples of students' work. To access this chapter's learning tools, go to ache.org/DecisionAnalysis and select Chapter 9.

analysis focuses on historical precedents and leaves organizations vulnerable to new and emerging threats. These are important criticisms of probabilistic risk analysis, and they are addressed in this chapter. In particular, examples are used to show that a focused analysis is surprisingly more practical than a comprehensive analysis. A focused analysis may be done in less time, even though it relies on objective data. Also, by using new probability tools, it is possible to estimate the chances that very rare events will occur. Although these estimates are not precise to the last digit, they are accurate in magnitude and provide a consistent method of tracking the probabilities of many rare events. Furthermore, the methodology can be extended to anticipate emerging threats, starting from a kernal of truth (a fact about an event that has happened) and extending scenarios of how similar events might happen elsewhere.

Definitions

Before proceeding, it is important to define various terms. *Risk analysis* assesses the probability of an adverse outcome—in this case, security violations. Included in this broad definition are terrorism, cyber attacks, and physical attacks. Risk analysis is not the same as threat analysis, however, in which the environment is scanned for credible attacks against the organization. Figure 9.1 shows the relationship between environmental threats, organization vulnerabilities, and security violations.

Organization vulnerability is an internal weakness that could, but does not always, lead to security violations. *Security controls* are business process changes and information technology steps that organizations can take to reduce their vulnerability or to mitigate the consequences of security violations. To conduct a *vulnerability assessment*, one needs to step back from actual security violations and look for causes of security violations. When a *security violation* occurs, there are often multiple causes for it. For example, a hacker or a cyber terrorist might be able to gain access to the organization's network through a disgruntled employee. Using this definition, penetration into the network is considered a security violation, the

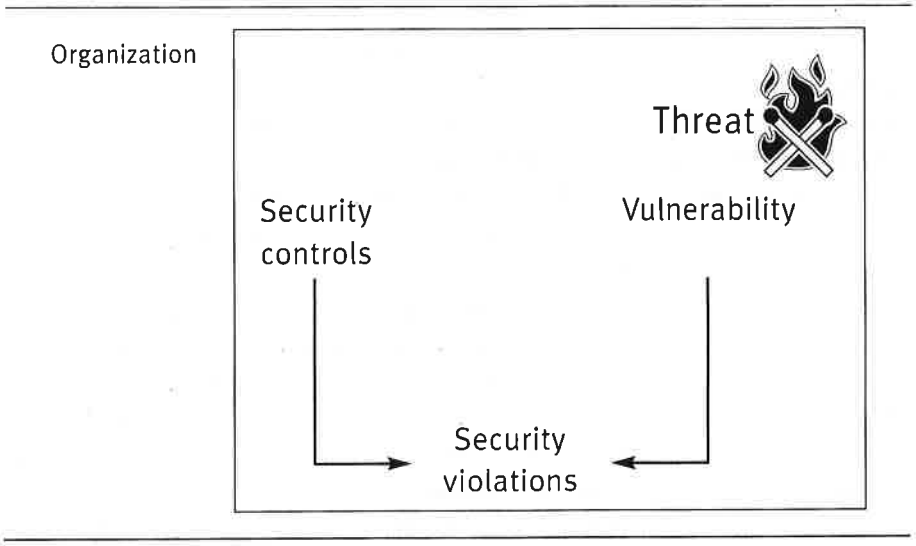

FIGURE 9.1 Threats, Vulnerability, and Security Violations

disgruntled employee is a vulnerability, and the hacker is the outside threat. In this sense, the risk analysis of security violations assesses the joint effect of threats, vulnerabilities, and security controls.

This chapter repeatedly refers to *security incidents.* A security incident is defined as "any action or event that takes place, whether accidental or purposeful, that has the potential to destabilize, violate, or damage the resources, services, policies, or data of the organization or individual members of the organization" (Rezmierski et al. 2005).

Analysis is the process of enumerating a set of scenarios for security violations (Kaplan and Garrick 1981). A focused risk analysis starts with objective data about security incidents and builds the scenarios around these incidents. Because it starts with actual incidents, the approach is also referred to as *objective risk analysis.* A *scenario* consists of one or more vulnerabilities that can lead to security violations. Examples of vulnerabilities include, but are not limited to, (1) discharging an employee without turning off access codes, (2) theft of computers, (3) attempted worm attacks, or (4) spy software on desktops. A *cyber security violation* is defined as network or desktop penetration by an outside agent independent of the intention.

History

In recent years, there have been many occasions in which risks for rare events have been assessed and subsequent events have helped confirm the

accuracy of the risk analysis or improve aspects of the analysis. Probabilistic risk analysis originated in the aerospace industry. One of the earliest comprehensive studies was started after the loss of life because of a fire in Apollo flight AS-204 in 1967. In 1969, the Space Shuttle Task Group in the Office of Manned Space Flight of NASA suggested that the probability of the loss of life should be less than 1 percent. Colglazier and Weatherwax (1986) conducted a probabilistic risk analysis of shuttle flights. But over time, NASA administrators abandoned the numerical forecast of risks because the projected risks were so high that they undermined the viability of the entire operation. Cooke (1991) and Bell and Esch (1989) report that NASA administrators "felt that the numbers could do irreparable harm" (Bell and Esch 1989). But subsequent shuttle accidents returned the emphasis on probabilistic risk analysis. Today, almost all components of space shuttles go through an independent risk analysis (Safie 1991, 1992, 1994; Planning Research Corporation 1989; Science Applications International Corporation 1995). A good example of such a risk analysis can be found in the work of Pate-Cornell and Fischbeck (1993, 1994); in this award-winning study, the authors link management practices to the risk that tiles on the shuttle will break away.

Probabilistic risk analysis has also been utilized to determine nuclear safety. Several studies have focused on reactor safety. The first such study was the reactor safety study conducted by the U.S. Nuclear Regulatory Commission (1975). The study was followed by a series of critical reviews (Environmental Protection Agency 1976; Union of Concerned Scientists 1977; Lewis et al. 1975), including a 1997 Congressional bill to mandate a review panel to examine the limitations of the study. The near failure of the reactor core at Three Mile Island, however, proved that the scenarios anticipated in the study were indeed correct, although the probability of human failures was underestimated. Not surprisingly, reviews of Three Mile Island emphasized the need for conducting a probabilistic risk analysis (Rogovin and Frampton 1980; Kemeny 1979). Kaplan and Garrick (1981) conducted a study of the probability of a reactor meltdown. The U.S. Nuclear Regulation Commission (1983) issued a manual for how to conduct a probabilistic risk analysis for the nuclear industry. Probabilistic risk analysis has also been used by energy firms that focus on sources of power other than nuclear power to predict catastrophic events (Cooke and Jager 1998; Rasmussen 1981; Ortwin 1998).

In addition to its use in the aerospace and nuclear industries, probabilistic risk analysis has also been applied to the prediction of a variety of natural disasters, including earthquakes (Chang, Shinozuka, and Moore 2000) and floods, as well as to the informed planning of coastal designs

(Voortman, van Gelder, and Vrijling 2002; Mai and Zimmerman 2003; Kaczmarek 2003). Probabilistic risk analysis has also been used to predict environmental pollution (Slob and Pieters 1998; Moore et al. 1999). A large number of studies have used probabilistic risk analysis to access waste disposal and environmental health (Ewing, Palenik, and Konikow 2004; Sadiq et al. 2003; Cohen 2003; Garrick and Kaplan 1999).

Probabilistic risk analyses are becoming increasingly utilized in healthcare organizations. In healthcare, probabilistic risk analyses have focused on root causes of sentinel adverse events, such as wrong-site surgery or failure mode and effect analysis of near catastrophic events (Bonnabry et al. 2005). Amgen Pharmaceutical has also used the procedure for making decisions regarding new product development (Keefer 2001). One difficulty in using probabilistic risk analyses for healthcare systems is the fact that in identifying and protecting against risks, organizations often rely on a rank orders and ignore the magnitude of the probability for a given adverse event (DeRosier et al. 2002).

New applications of probabilistic risk analyses are being used with respect to terrorism. Taylor, Krings, and Alves-Foss (2002) have applied a probabilistic risk analysis to assessing cyber terrorism risks. Others have suggested using these techniques in assessing other types of terrorism (Apostolakis and Lemon 2005; Haimes and Longstaff 2002).

Procedures for Conducting a Focused Risk Analysis

Step 1: Specify Decisions to Be Made

Before analyzing risks, an organization needs to clarify how the risk assessment will be used. For example, an organization might want to use the risk assessment to allocate the budget for security controls. If the assessment finds that the organization is most vulnerable to a cyber attack, then money can be spent on improving the security of its computers. If the organization finds that employees' departures from the organization are leading to many security violations, then more money may be spent on improving this process. The point is that it should be clear what choices are available to the chief security officer. It should also be clear how security assessments can lead to corrective action.

Step 2: Organize an Incident Database

A focused risk analysis starts with historical precedence and adds to this list additional information about emerging threats. It assumes that history repeats itself and that the first place to anticipate the future is by examining

the recent past. This is done by organizing a *security incident database.* An incident database lists the security violation, its date of occurrence, and the risk factors or vulnerabilities that led to it.

An incident database of security violations is used to collect data from one participant and report it to all others. In this fashion, participants have access to patterns of violations across the industry. First, participants register and sign a consent form. Then, participants are asked to report the security violations within their organization, including the date of the violation.

In this fashion, as more participants contribute data to the incident database, a list of types of security violations and their contributing causes emerges. In focused risk analyses, an incident database is used in two ways. First, it is used to focus the investigation on the types of violations and vulnerabilities listed in the database. Because this list is by definition more limited than comprehensive lists of what could possibly lead to security violations, focused analysis radically reduces the effort needed for conducting a risk analysis. The incident database is also used to assess the frequency of security violations, as well as the relationship between the security violation and various vulnerabilities.

Examples of incident databases abound. The Symantec Corporation collects and reports the largest database of cyber attacks.[2] This database of incidents can be used to assess the conditional probability of a security violation given specific cyber vulnerabilities. Another example is the National Vulnerability Database, which also maintains a listing of incidents of cyber security vulnerabilities.[3]

A broad example of security violations can be found in voluntary databases maintained by associations. For example, the Joint Commission on Accreditation of Healthcare Organizations (JCAHO) has created a database for voluntarily reported incidents of sentinel events (e.g., medication errors or wrong-site surgery). If JCAHO would consider security violations to be sentinel events, then its database could serve as the repository for this proposed incident database.

Incident databases can be constructed from publicly available data. For example, Alemi and Arya (2005) needed an incident database for unauthorized disclosures. They identified publicly available reports of unauthorized disclosures from (1) reviews of complaints to the U.S. Department of Health and Human Services regarding privacy issues, and (2) legal and news databases for reports of unauthorized disclosures. Table 9.1 shows the terms used to search for unauthorized disclosures and the number of unique cases found.

It is possible, and perhaps likely, that there exist other cases in which unauthorized disclosures have occurred. Public sources do not include

TABLE 9.1
Frequency of Publicly Reported Incidents of Unauthorized Disclosures

Terms Searched	*Databases Searched*	*Records Found*	*Number of Unauthorized Disclosures*	*Dates*	*Probability of Unauthorized Disclosure*
Patient confidentiality [keyword]; OR confidential medical records [keyword]; OR privacy [keyword]; medical records [additional terms]; OR privacy [keyword]; medical records [additional terms]; unauthorized disclosure [focus]	LexisNexis Academic	47	2	01/01/03–12/31/03	.005
Privacy of [subject] cases [subdivision]; OR medical records [subject] cases [subdivision]; OR medical records [subject] laws, regulations, and rules [subdivision]; OR hospital information systems [subject] safety and security measures [subdivision]	Health Reference Center-Academic Infotrac	141*	8	01/01/90–12/31/03	.022
U.S. Department of Health and Human Services; HIPAA complaints	DHHS reports	22	16	01/01/03–12/31/03	.044
Direct reports		3	3	01/01/03–12/31/03	.008
Total:		213	29	01/01/90–12/31/03	.079

* Also includes additional journal reports of unauthorized disclosure.

many of the private incidents. Therefore, their list of security violations and related risk factors might be incomplete. But no matter how many cases are reviewed, the number of risk factors will be relatively small because many risks can be imagined but few actually occur. Because relying on case histories reduces the number of risk factors, it reduces the time it takes to conduct a risk analysis.

In some industries, public incident databases are not available. If an incident database does not exist, it is possible to collect one through industry contacts. A handful of organizations can collaborate and share security violations across their organizations and thus start a small incidence database. This certainly would not be a complete list of violations, but it is better than having no data at all. Obviously, any incident database becomes more accurate as a larger percentage of security violations are reported. The more data, the more the security assessment is grounded in reality.

Step 3: Estimate the Probability of Security Violations

There are two ways to estimate probability of future security violations: direct and indirect methods. The latter method estimates probability of security violations from various vulnerabilities and risk factors within the organization. The former method estimates it from past patterns of violations. Both methods are described below in more detail.

Direct Method

The next step is to use the incident database to estimate the probability of various types of security violations. Security violations are often rare, and the incident database may contain only one or two examples of such violations. Furthermore, the probability of the violations cannot be estimated from experts' or employees' recall because, when it comes to describing rare events, people have a hard time talking about or keeping track of small probabilities.

Psychological research has shown that people often exhibit selective memory bias for events that are personally relevant (Ellwart, Rinck, and Becker 2003; Becker, Roth, and Andrich 1999; Gardner, Pickett, and Brewer 2000). In addition, emotionally arousing events often cause individuals to recall the event with greater detail and specificity (Schmidt 2004; Cahill and McGaugh 1998). Often, rare security events are personally relevant to many and are of an emotionally arousing nature. A situation in which a hospital is attacked by terrorists who kill hundreds of helpless patients is very personally relevant, even to those unaffected directly by the attack, because such an event exposes everyone's vulnerability. By the same token, witnessing such an event, either firsthand or through news coverage, causes extreme feelings of sorrow, fear, and anger. These factors will cause such events to stick out in people's minds and distort their understanding of the probability of such an attack. Memories

of such events will be more salient and vivid than for other events. In sum, people are bad at accurately estimating the probability of rare security events.

Surprisingly, experts can describe with considerable confidence the time to the event. For example, many have difficulty referring to or imagining the probability of 0.000274, but they may easily make statements such as "this event has occurred once in the last decade." Because experts and employees have an easier time thinking of rare events in terms of the time to the event as opposed to a frequency count, one way to estimate probability of rare security events is through the time to the event.

If one assumes that an event has a Bernoulli distribution (i.e., the event either happens or does not happen; it has a constant daily probability of occurrence; and the probability of the event does not depend on prior occurrences of the event), then the time to the next occurrence of the event has a geometric distribution. In a geometric distribution, the probability of a rare event, P, can be estimated from the average time to the occurrence of the event, T, using the following formula:

$$P = \frac{1}{1 + T}.$$

In this approach, the frequency of an event is first estimated by calculating the time to reoccurrence of the event. For example, investigators often assume an event happens daily, weekly, monthly, once a year, once every two years, once every five years, or once a decade. This time to the event can be transferred to a frequency count using the above formula (see Table 9.2).

Some security violations are so rare that they may not occur during the observation period at all, or they may occur only once. In these

TABLE 9.2 Calculated Probabilities for Various Terms

Word Assignment	*Frequency of Event*	*Calculated Probability*
Negligible	Unlikely to occur*	0.0003
Very low	2–3 times every 5 years	10.0014
Low	≤ once per year	0.0027
Medium	≤ once every 6 months	30.0056
High	≤ once per month	0.0055
Very high	> once per month**	0.1429
Extreme	> one per day	1.0000

* Assumes less than once every 10 years
** Assumes once per week

circumstances, the length of the observation period can be used as a surrogate for the time between reoccurrences. This assumes that the security violation would occur the day after the end of the observation period, and thus it provides an upper limit for the prevalence of the security event. For an example of the use of the formula, consider that you want to assess the prevalence of physical theft of a computer. Suppose your records show that such theft occurs once every three months; then the time between two thefts is 90 days, and the probability of a theft for any day is calculated as

$$P(\text{Physical theft of a computer}) = \frac{1}{1+91} = 0.01.$$

Another method of improving the accuracy of estimates of rare events is to purposefully examine the event in artificially constructed samples where the event is not rare (Heidelberger 1995). Then the frequency of the event in the sample can be extrapolated to the remaining situation proportional to how narrowly the sample was drawn. The procedure is generally known as "importance sampling" and involves sampling data from situations where one expects to find the rare event. Assume that you have taken m narrowly defined samples, and sample i represents W_i cases in the population of interest. If P_i is the probability of the event in the narrowly defined sample, then the probability of the rare event, P, can be calculated as

$$P = \frac{\sum_{i=1,\ldots,m} W_i \times P_i}{\sum_{i=1,\ldots,m} W_i}.$$

An example may demonstrate this concept. Suppose you want to estimate the probability that electronic data could be stolen by someone overcoming the password protection in a computer. For most organizations, such an attack is rare, but the attack is more likely to be seen in computers that are infected by a virus. Suppose that in an organization, one in 100 computers has a major virus. Also suppose that the examination of data trails in these infected computers shows that 0.3 percent involve a loss of data. What is the probability of the loss of data anywhere in the organization? This probability is calculated by weighting the narrow sample of infected computers to reflect the proportion of these computers inside the organization:

$$P = \frac{1}{100} \times 0.003 + \frac{99}{100} \times 0.$$

Note that in this calculation it is assumed that a loss of data does not occur in computers without a virus infection. This may be wrong but, as a first approximation, may be reasonable, because it is anticipated that

most data loss occurs among infected computers. The importance weighting procedure requires one to know a priori, with a high level of certainty, both the conditions under which the rare event are more likely to occur and the prevalence of the conditions.

Indirect Method

In the indirect approach, the probability of security violations is estimated from the presence of various vulnerabilities and risk factors within the organization. A survey is constructed based on the risk factors identified across the industry through the incident database. Then, the organization's employees are surveyed regarding practice patterns in their midst, and data from the survey and incident database are used to estimate the probability of future security violations using the following formula:

$$P(V|R_1, \ldots, R_n) = \sum_{i=1,\ldots,n} P(V \mid R_i) \times P(R_i).$$

where

- n is the number of hazards;
- R_i is the risk factor i;
- $P(V \mid R_1, \ldots, R_n)$ is the probability of security violations given various risk factors (vulnerabilities) in the organization;
- $P(V \mid R_i)$ is the conditional probability of security violations given the presence of a risk factor in the organization. This variable is calculated using the Bayes's theorem presented below; and
- $P(R_i)$ is the prevalence of the risk factor in the organization. This variable is calculated from the time to occurrence of the events (see below).

This formula is known as the *law of total probability*, and it states that the probability of a security violation is the sum of all the ways in which a security violation can happen from different risk factors (see Chapter 3).

The frequency of risk factors within an organization, $P(R_i)$, is estimated by surveying key informants within the organization. As risk factors can also be rare, one should assess the probability of their presence from the average time between reported occurrences of the risk factor. As before, use of this formula assumes that the risk factor has a binomial distribution of occurrence, in which the probability of the risk factor is relatively rare but is constant and independent from future occurrences. These assumptions may not be reasonable. For example, when organizations actively improve their security, the assumption of constant probability is violated. If the assumptions of binomial distribution are met or are acceptable as a first approximation, then the time between the presence of risk factors has a geometric distribution, and the formula presented earlier can be used.

Bayes's theorem is used to calculate the probability of unauthorized disclosure after the occurrence of a risk factor:

$$P(U \mid R_i) = \frac{P(R_i \mid U) \times P(U)}{P(R_i)}$$

where

- $P(R_i)$ is the probability of observing risk i. This is obtained from surveys of healthcare organizations using time to occurrence of the risk factor;
- $P(U)$ is the probability of unauthorized disclosure across institutions. These data are calculated from the Incidence Database of Unauthorized Disclosures; and
- $P(R_i|U)$ shows the prevalence of risk factor i among unauthorized disclosures. These data are also available from the Incidence Database on Unauthorized Disclosures.

An example of how to apply the indirect method can be shown using the privacy incident database reported earlier (Alemi and Arya 2005). To start with, a master list of privacy violations was created from the incidence database (see Table 9.3). Four hospitals were surveyed using this master list. Table 9.3 also contains the probability of each risk factor as well as the prevalence of the security violation given the risk factor.

The overall privacy risk for the organization listed in Table 9.3 was calculated as 0.01. Table 9.4 provides the same probability at different organizations. The data in Table 9.4 can be used as benchmarks for comparing various hospitals. For example, the data show that the risk at Hospital 2 is lower than the risk at Hospital 1.

Step 4: Adjust the Probability of Security Violations Based on Incidents Elsewhere

In the previous steps, the analyst has estimated the probability of security violations within the organization based on historical incidents. To make this estimation more accurate, the analyst must adjust the probability to reflect emerging threats. These emerging threats have not occurred in the industry but have occurred elsewhere in other industries, and there are concerns that the situations are similar enough that they may occur in the organization being assessed. Here again is a kernel of truth around which the analyst might construct a speculative scenario about what might happen within the organization if the event were to occur there.

The adjustment for emerging threats can be made using the method of similarity judgment. Similarity judgment involves predicting an event

TABLE 9.3 Predicting Probability of Violations from Prevalence of Vulnerabilities

Description of Risk Factor	*Prevalence of Risk Factor in the Organization*	*Prevalence Security Violation Given the Risk Factor*
Employee views paper documents or manipulates computer passwords to view records of patients not under her care	0.0003	1
Benefit organizations or employers request employee information	0.0003	0.8805
Employees engage in whistle blowing to uncover illegal or unacceptable business or clinical practices	0.0003	0.0201
Clinician uses unsecured e-mail environment	0.0003	0.1606
Employee removes patient records from secure location or workplace without authorization	0.0003	0.88
External infection of computers/password/ network systems (e.g., computer hacker)	0.0003	0.5888
Theft of computers or hard drives	0.0003	0.5867
Sale of patient records	0.0003	1
Blackmail or extortion of organization or an employee	0.0003	1
Changes in custody or family relationships not revealed by the patient	0.0003	0.1472
Audit of business practices by outside firm without clinicians' approval	0.0003	0.4416
Business associate violates chain of trust agreement	0.0003	1
Error in patient identity during data transfer to third-party insurers	0.0014	0.0142
Caring for employees' friends and family members and discussing the care outside of the work environment	0.0014	0.2202
Clinician gathers information from patients' family and friends after the visit without the patient's consent	0.0014	1
Patient uses identity of another person to gain insurance benefits	0.0056	0.093
Patient records (paper documents) not sealed or kept in secure environment	0.0056	0.0592
Discussion of patient care with coworkers not engaged in care	0.0056	0.1218
Medical reports or records with wrong recipient information	0.1429	0.0405
Patient care discussed in a setting where others can easily hear	0.1429	0.0023

TABLE 9.4 Overall Risk of Privacy Violations Calculated from Various Vulnerabilites Within Four Organizations

	Hospital 1	*Hospital 2*	*Hospital 3*	*Hospital 4*
Rate of security violations	0.022	0.011	0.011	0.012

based on the historical precedence of a similar event. For example, before the September 11 attack on the World Trade Center in New York City, terrorists tried to attack the Eiffel Tower by flying a hijacked plane into it. The two incidents are similar in the sense that both are tall buildings with important symbolic value. Both were attacked using a passenger jet in the hopes that the jet fuel would lead to additional destruction. They are, of course, also different incidents occurring for different reasons at different times in different places. Based on the pattern of shared and unshared features between the two events, the analyst can calculate the probability that the novel event will occur. Similarity judgments can be used to extend the probability of known rare events to new situations.

Psychologists have conducted numerous experiments showing that the similarity of two situations will depend on features they share and features unique to each case (Mobus 1979). In 1977, Tversky summarized the research on similarity and provided a mathematical model for judging similarity. The similarity of two situations, i and j, can be assessed by listing the following three categories of features:

1. Features in the index case but not in the prototype, $f_{i,\text{ not } j}$;
2. Features in the prototype but not in the index case, $f_{\text{not } i,\, j}$; and
3. Features in both cases, f_{ij} .

Then similarity, S, can be measured as the count of shared and not shared features using the following formula:

$$S_{ij} = \frac{f_{ij}}{f_{ij} + a(f_{i,\text{ not } j}) + b(f_{\text{not } i,\, j})}.$$

In above formula, the constants a and b add up to 1 and are set based on whether the index case is a defining prototype. If these constants are different from 0.5, they allow the comparison case to be more like the index case than vice versa.

Once an estimate of similarity of the index case and the prototype are available, then the probability of an attack in the index case can be calculated as

$$\text{Probability of attack in index case} = \text{Probability}_{\text{prototype}} \times \text{Similarity}_{\text{case, prototype}}.$$

For example, recall the Beslan school siege in North Ossetia, Russia in September 2004. Every year on the first day of September, every school in Russia celebrates the holiday known as the Day of Knowledge. The children dress in their finest clothes and are accompanied to school by parents and other family members. On this particular holiday, 30 Chechen rebels used this tradition as an opportunity to seize the school and take more than 1,300 hostages. The siege ended two days later when Russian Special Forces stormed the building. The crisis left more than 330 civilians dead, 186 of whom were schoolchildren, and hundreds wounded.

Suppose you want to estimate the probability of a Beslan-like siege on a hospital in the United States. Using the method of similarity judgment, a risk analyst would ask, "What is the likelihood of a terrorist attack on schools in Russia?" Next would follow the question, "How similar are the conditions in Russia and the United States?" By judging the probability of an actual event and the similarity of that event to conditions existing in the United States (e.g., hospital populations), the likelihood that a hospital would be the target of a similar terrorist attack can be estimated.

The Beslan school siege is considered a prototype of how vulnerable children might be gathered and killed. Because such an attack has only occurred only once from September 2004 to May 2006, its probability of reoccurring is estimated to be 0.0009. The risk analyst needs to determine the features that a school in Russia shares with a hospital in the United States, as well as those features unique to each setting. The school and the hospital are similar in the sense that both are buildings that house a sizable number of civilians, both serve a vulnerable population, and both are publicly accessible. Here is one summary of shared and different features in the two situations:

1. Features in the index case (school) but not in the comparison case (hospital):
   a. No proximity defense
   b. No communication system available between rooms
   c. Capacity to house population into one central location
   d. School-age children
2. Features in the comparison case (hospital) but not in the index case (school):
   a. Difficulty in gathering the population into one central location
   b. Availability of security officers
   c. Presence of items that could be used for defense
3. Features shared by both cases:
   a. Large number of civilians
   b. Vulnerable population

c. Publicly accessible

This list is for the purpose of providing a brief example; obviously, additional analysis might reveal more features. Here it is assumed that the constant a is 0.20 and the constant b is 0.80, because the similarity between the two situations are quite asymmetrical. The attack on the hospital is more likely to be judged similar to the Beslan school siege than the Beslan school siege is likely to be judged similar to the attack on the hospital. The similarity of the hospital situation to the Beslan school situation is calculated as

Based on this measure of similarity of the two situations,[4] the probability of a similar attack on the hospital is calculated as

$$\text{Similarity}_{\text{hospital, Beslan school}} = \frac{3}{3+(0.20\times 4)+(0.80\times 3)} = 0.48.$$

$$\text{Probability of similar attack on hospital} = \text{Probability}_{\text{Beslan attack}} \times \text{Similarity}_{\text{hospital, Beslan,}}$$

$$\text{Probability of similar attack on hospital} = 0.0009 \times 0.48 = 0.0004.$$

Step 5: Report Findings to the Organization

In the final report, the probability of various types of security violations, including emerging threats, are reported. This report should identify the credible threats faced by the organization, as well as set priorities among risks to guide the organization in its preventive efforts.

A Case Example

Suppose an analyst was asked to estimate the overall risks faced by a nursing college in a university in the southern United States. In step one, the analyst articulated the decisions faced by the nursing college. These included the following:

1. Should more funds be put into protecting against computer viruses?
2. Should faculty and staff be educated about physical security and theft?
3. Should background checks be required for all prospective nursing students?
4. Should a camera surveillance of offices be implemented?

In step two, an incident database was constructed from events that had occurred at the university in the past five years. Because of the limited

nature of this incident database, the analysis should be considered preliminary until confirmed against incidents in other universities. The analyst had access to dates of occurrences of various physical security incidents with the university, but the database did not contain information on computer security violations. The observed data for physical incidents was used, and the analyst supplemented it with employee's estimated rates for the time to the next information technology (IT) security incidence.

The IT risk factors for the nursing college were classified into the groupings suggested by a research study (Rezmierski et al. 2005). The employee in charge of security incidents at the nursing college was asked to estimate the number of days to various incidents, and this information was used to estimate the rates of various incidents. Table 9.5 shows the risk factors, estimated days to the event, and estimated frequency.

TABLE 9.5 Example of IT Security Violations

IT Security Violation	*Description and Possible Risk Factors*	*Estimated Days to Event*	*Probability*
Desktop security violations	This may be caused by failure to install relevant operating system or application software patches or failure to have updated virus protection. An example is the GAO Bot Outbreak.	3 months	.03
Unsolicited e-mails requesting personal information	Employees receive disguised alerts from well-known companies (e.g., a bank) requesting them to send information in order to (1) complete an application, (2) prevent a security breach, or (3) win money.	Once a week	.14
Unsolicited e-mails not requesting personal information	Employees receive e-mails advertising products. Sender's machine has guessed the employee's e-mail or has obtained the e-mail through the web. No private information is asked for. Strictly speaking, this is not a security violation but is listed here because of its potential to lead to large numbers of employees falling victim to financial scams.	Daily	1.00
Network penetration	Outside hacker obtains illegal access to the network by manipulating the system or purchasing passwords from disgruntled employees	Once in last two years	.0014

In step three, the probability of various security violations was calculated. For each security violation, the time to the event was transferred into a frequency count. For example, in the past two years, there was one occasion in which a person was able to gain access to the information on the servers. Therefore, the probability of network penetration was calculated as follows:

$$P(\text{Network penetration}) = \frac{1}{2 \times 365 + 1} = 0.0014.$$

To assess the non-IT risks for this nursing college, the analyst used the data in the five-year incidence database. Table 9.6 shows the various non-IT security violations and the dates of their occurrences.

The frequencies of events in Table 9.6 were calculated from actual observations of dates of the events in the previous five years at the university. For example, Table 9.7 shows the steps in calculating daily probability of computer theft.

First, the dates of computer theft were sorted. Then, the difference between two consecutive dates was calculated. Next, the differences were averaged to produce the average number of days until the next occurrence of the incidence. Finally, the days to the next occurrence were used to calculate a daily rate.

In step four, emerging risks were added in. The analysis was supplemented with information about shootings at the University of Arizona (UA). On Monday, October 28, 2002, Robert Flores, a nursing student

TABLE 9.6 Observed Frequencies of Security Violations

Category of Risk Factor	*Number of Incidents*	*First Reported Date*	*Last Reported Date*	*Average Days Between Occurrences*	*Daily Rate*
Theft of computer	21	7/1/1999	11/29/2004	99	0.010
Theft of other equipment	36	2/5/1999	8/10/1999	63	0.016
Theft of personal property	2	7/12/2001	7/11/2003	365	0.003
Property damage	26	10/7/1999	10/7/2004	73	0.013
Vehicle accident on premise	10	10/27/2000	8/3/2005	193	0.005
Damage from natural causes incidents	40	12/26/1999	6/30/2005	52	0.019
hazardous materials	1	10/10/2003	10/10/2003	726	0.001

TABLE 9.7 Sample Calculation of Daily Rate of Security Violations

Date of Theft of Computers	*Time Between Consecutive Thefts**
7/1/1999	14.00
7/15/1999	146.00
12/8/1999	55.00
2/1/2000	191.00
8/10/2000	34.00
9/13/2000	133.00
1/24/2001	231.00
9/12/2001	86.00
12/7/2001	26.00
1/2/2002	64.00
3/7/2002	141.00
7/26/2002	52.00
9/16/2002	16.00
10/2/2002	147.00
2/26/2003	257.00
11/10/2003	128.00
3/17/2004	97.00
6/22/2004	31.00
7/23/2004	5.00
7/28/2004	124.00
11/29/2004	—

Average time between thefits	98.900
Standard deviation	73.421
Count of events	21
Daily rate	0.010

at UA, who apparently was angry at having been barred from taking a midterm exam, entered the classroom where the exam was taking place and shot and killed two professors. It was discovered later that a third nursing professor had also been killed in her office on another floor of the building. After killing his professors, the student killed himself. According to reports of nursing staff and fellow students (Rotstein 2002), the student often tangled with professors and disrupted class by asking inappropriate questions and challenging teachers. In the weeks leading up to the shooting, the student had failed one class and was in danger of failing a second. In April of 2001, a nursing staff member reported to the university police that the student had conveyed to staff that he was depressed and suicidal, and that he may take action against the College of Nursing in retaliation for the perceived lack of respect and assistance he received from his professors. Others also reported that the student had bragged about obtaining a

concealed weapons permit. In a letter sent to the *Arizona Daily Star* before his death, the student reported a troubled childhood and stated that he was experiencing a great deal of stress in his personal life because of health problems and a recent divorce. He described being pushed to the breaking point by his recent poor performance at school and the possibility that he would fail out of the nursing program.

This incident caused many universities to reexamine security strategies, fearing a similar attack on their campuses. Before a university expends large amounts of time, effort, and money toward preventing such an attack, however, it would be useful to assess the likelihood that such an attack may occur on campus. The method of similarity judgment was used to estimate the likelihood of this incidence at the nursing college in this case example. To estimate the likelihood of a shooting at the nursing college, the analyst first needed to determine the likelihood of reoccurrence of the UA shooting. Next, the analyst needed to assess the similarity of the conditions between the nursing college and UA.

The probability of reoccurrence of the UA shooting was estimated to be at least once in the past four years (0.0007). Next, the analyst identified the features that the nursing college shares with UA, as well as those features unique to each setting.

Recall the formulation of the similarity between the two schools:

1. Features in UA but not in the nursing college, $f_{\text{UA, Not college}}$:
   a. Large enrollment (61,000 students)
2. Features in the nursing college but not UA, $f_{\text{College, Not UA}}$:
   a. Mostly working students
   b. Potential students screened with a background check
3. Features shared by both colleges, $f_{\text{College, UA}}$:
   a. Easily accessible
   b. Large population of students, faculty, and staff
   c. Campus police
   d. Standards for student academic performance
   e. Focus on nursing or health science

The analyst measured similarity using the count of shared and not shared features:

$$S_{\text{College, UA}} = \frac{f_{\text{College, UA}}}{f_{\text{College, UA}} + (a \times f_{\text{College, Not UA}}) + (b \times f_{\text{UA, Not College}})}$$

The analyst used the estimate 0.20 for the constant a and the estimate 0.80 for constant b. The similarity of the nursing college situation to the UA situation was calculated as

$$\text{Similarity}_{\text{College, UA}} = \frac{5}{5 + (0.20 \times 1) + (0.80 \times 2)} = 0.74.$$

To calculate the probability of a similar event occurring at the nursing college, the analyst multiplied the probability of the UA shooting reoccurring by the similarity between UA and the nursing college:

$$\text{Probability of school shooting at nursing college} = 0.0007 \times 0.74 = 0.0005.$$

In the final step, a report should prepared for the nursing college's leadership group, providing them with the list of security violations. The leadership group was asked to think through the relative frequency of various violations and decide how to distribute their limited security funds.

Summary

Recall the three criticisms of objective focused risk assessment: rare probabilities cannot be estimated, probabilistic analysis is too time consuming, and emerging threats will be missed. These criticisms are not valid. It has been shown by way of examples that it is easy and practical to assess the probability of rare events through the use of various probability tools (e.g., time to event, importance sampling). It has also been shown that emerging new threats can be added to the analysis through similarity judgments.

Focused risk analysis has a distinct advantage over comprehensive and consensus-based approaches: it is more grounded in reality, and is not based on speculations regarding potential risks but on actual experienced incidents within the enterprise and across the industry. In this fashion, the proposed approach may be more accurate than a consensus-based approach. Credible threats can be identified from actual incidents, allowing organizations to set realistic priorities in their efforts to protect against security and privacy violations.

The focused risk assessment is based on analysis of actual incidents within the industry or outside it; in this sense, it starts with a kernel of truth. An incident database is used to focus the assessment on risk factors that have occurred in at least one other healthcare organization or elsewhere in the world. In contrast, comprehensive and consensus-based assessments are often based on imagined risks that might mislead organizations to protect against events that may never occur. In doing so, they may waste precious security funds. Even worse than a one-time waste is the prospect that when another consultant, with a more active imagination and a more

vivid assessment tool, shows up, the healthcare organization is catapulted to invest more—chasing elusive and esoteric security targets. Because imagination is limitless, there is no end to how much should be spent on security and which vulnerability is more important. Like a child, the organization ends up fighting imaginary foes. Risk assessment, instead of helping the organizations focus on high-value targets, misleads them to pursue irrelevant targets. When analysis is based on real vulnerabilities and threats, an organization can focus on probable risks and rationally prioritize and limit investment in security controls.

Review What You Know

1. How can the probability of a rare event be measured? Describe at least two methods for doing so.
2. If an event occurred once five years ago, what is its minimum daily probability of occurrence?
3. Suppose last year, computer thefts occurred on March 10, September 1, and October 6 in your organization; what is the average number of days to reoccurrence of the computer theft? How will your estimate of the average length of days to computer theft be different if you assume that there will be a theft at start of next year on January 1. What is the daily probability of occurrence of computer theft (give a range based on your different assumptions)?
4. Calculate the probability that a shooting will occur within a hospital by reviewing media reports on the web regarding these incidents. List the dates of the shootings and calculate the probability of the time to the event.

Rapid-Analysis Exercises

Assess the probability of unauthorized disclosure and security violations at one hospital and clinic by following these steps:

1. Interview at least one person in the organization to collect data on prevalence of various risk factors using the instrument available at the Chapter 9 section of this book's companion web site at ache.org/DecisionAnalysis.
2. Use time between events to assess the daily prevalence of risk factors.
3. From the information on industry patterns in Table 9.3, estimate the overall probability of unauthorized disclosure for your hospital or clinic.

TABLE 9.8 Worksheet for Reporting Risks

Category of Risk Factor	*Number of Incidents*	*First Reported Date*	*Last Reported Date*	*Average Days Between Occurrences*	*Daily Rate*
Theft of computer					
Theft of other equipment					
Theft of personal property					
Property damage					
Vehicle accident on premise					
Damage from natural causes					
Hazardous materials incidents					
Desktop security violations					
Unsolicited e-mails requesting personal information					
Unsolicited e-mails not requesting personal information					
Network penetration					

4. For your organization, interview your contact person and record responses on Table 9.8.
5. Use the information in the first four rows of the table to calculate the daily probability of various types of security violations.
6. Provide a report on what should be the top three priorities of the clinic or hospital.

Audio/Visual Chapter Aids

To help you understand the concepts of security-risk analysis, visit this book's companion web site at ache.org/DecisionAnalysis, go to Chapter 9, and view the audio/visual chapter aids.

Notes

1. This research was supported in parts by the National Capital Region Critical Infrastructure Project (NCR-CIP), a multi-university consortium managed by George Mason University, under grant #03-TU-03 by the U.S. Department of Homeland Security's Urban Area Security Initiative, and grant #2003CKWX0199 by the U.S. Department of Justice's Community Oriented Policing Services Program. The views expressed are those of the authors, and do not necessarily reflect those of the Department of Homeland Security or the Department of Justice.

2. See http://www.symantec.com/index.html.

3. See http://nvd.nist.gov.

4. Please note that this is not the same as the similarity of the Beslan school incident to the hospital situation, which is

$$\text{Similarity}_{\text{Beslan school, hospital}} = \frac{3}{3 + (0.20 \times 3) + (0.80 \times 4)} = 0.44.$$

References

Alemi, F., and V. Arya. 2005. "Objective Analysis of Privacy Risks." [Online information; retrieved 11/7/2005]. http://gunston.doit.gmu.edu/healthscience/730/RiskAnalysis.asp.

Apostolakis, G. E., and D. M. Lemon. 2005. "Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism." *Risk Analysis* 25 (2): 361–76.

Becker, E. S., W. T. Roth, and M. Andrich. 1999. "Explicit Memory in Anxiety Disorders." *Journal of Abnormal Psychology* 108 (1): 153–163.

Bell, T. E., and K. Esch. 1989. "The Space Shuttle: A Case Study of Subjective Engineering." *IEEE Spectrum* 26 (6): 42–6.

Bonnabry, P., L. Cingria, F. Sadeghipour, H. Ing, C. Fonzo-Chrite, and R. E. Pfister. 2005. "Use of a Systematic Risk Analysis Method to Improve Safety in the Production of Pediatric Parenteral Nutrition Solutions." *Quality Safety Health Care* 14 (2): 93–8.

Cahill, L., and J. L. McGaugh. 1998. "Mechanisms of Emotional Arousal and Lasting Declarative Memory." *Trends in Neuroscience* 21 (7): 194–9.

Chang, S. E., M. Shinozuka, and J. E. Moore. 2000. "Probabilistic Earthquake Scenarios: Extending Risk Analysis Methodologies to Spatially Distributed Systems." *Earthquake Spectra* 16 (3): 557–72.

Cohen, B. L. 2003. "Probabilistic Risk Analysis for a High-Level Radioactive Waste Repository." *Risk Analysis* 23 (5): 909–15.

Colglazier, E.W., and R. K. Weatherwax. 1986. "Failure Estimates for the Space Shuttle." In *Abstracts for Society Analysis Annual Meeting*, 80. McLean, VA: Society for Risk Analysis.

Cooke, R. M. 1991. *Experts in Uncertainty: Opinion and Subjective Probability in Science.* New York: Oxford University Press.

Cooke, R. M., and E. Jager. 1998. "A Probabilistic Model for the Failure Frequency of Underground Gas Pipelines." *Risk Analysis* 18 (4): 511–27.

DeRosier, J., E. Stalhandske, J. P. Bagain, and T. Nudell. 2002. "Using Health Care Failure Mode and Effect Analysis: The VA National Center for Patient Safety's Prospective Risk Analysis System." *Joint Commission Journal of Quality Improvement* 28 (5): 248–67.

Ellwart, T., M. Rinck, and E. S. Becker. 2003. "Selective Memory and Memory Deficits in Depressed Inpatients." *Depression and Anxiety* 17 (4): 197–206.

Environmental Protection Agency. 1976. *Reactor Safety Study Oversight Hearings before the Subcommittee on Energy and the Environment of the Committee on Interior and Insular Affairs, House of Representatives.* 94th Cong., 2d sess., June 11.

Ewing, R. C., C. S. Palenik, and L. F. Konikow. 2004. Comment on "Probabilistic Risk Analysis for a High-Level Radioactive Waste Repository" by B. L. Cohen. *Risk Analysis* 24 (6): 1417.

Gardner, W. L., C. L. Pickett, and M. B. Brewer. 2000. "Social Exclusion and Selective Memory: How the Need to Belong Influences Memory for Social Events." *Personality and Social Psychology Bulletin* 26 (4): 486–96.

Garrick, B. J., and S. Kaplan. 1999. "A Decision Theory Perspective on the Disposal of High-Level Radioactive Waste." *Risk Analysis* 19 (5): 903–13.

Gray, G. M., and D. P. Ropeik. 2002. "Dealing with the Dangers of Fear: The Role of Risk Communication." *Health Affairs* 21 (6): 106–16.

Haimes, Y. Y., and T. Longstaff. 2002. "The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism." *Risk Analysis* 22 (3): 439–44.

Heidelberger, P. 1995. "Fast Simulation of Rare Events in Queueing and Reliability Models." *ACM Transactions on Modeling and Computer Simulation (TOMACS)* 5 (1): 43–85.

Kaplan, S., and B. J. Garrick. 1981. "On the Quantitative Definition of Risk." *Risk Analysis* 1 (1):11–27.

Kaczmarek, Z. 2003. "The Impact of Climate Variability on Flood Risk in Poland." *Risk Analysis* 23 (3): 559–66.

Keefer, D. L. 2001. "Practice Abstract." *Interfaces* 31 (5): 62–4.

Kemeny, J. 1979. *Report of the President's Commission on the Accident at Three Mile Island.* Washington, DC: Government Printing Office.

Kollar, J. J., B. C. Lipton, W. T. Mech, A. D. Pelletier, D. S. Powell, E. C. Shoop, R. S. Skolnik, G. G. Venter, D. L. Wasserman, T. A. Weidman, and S. Ringsted. 2002. *Terrorism Insurance Coverage in the Aftermath of September 11th.* Washington, DC: American Academy of Actuaries. [Online report; retrieved 10/11/05] http://www.actuary.org/pdf/casualty/terrorism_may02.pdf.

Leask, A., V. Delpech, and J. McAnulty. 2003. "Anthrax and Other Suspect Powders: Initial Responses to an Outbreak of Hoaxes and Scares." *New South Wales Public Health Bulletin* 14 (11–12): 218–21.

Lewis, H. W., R. J. Budnitz, A. W. Castleman, D. E. Dorfan, F. C. Finlayson, R. L. Garwin, L. C. Hebel, S. M. Keeny, R. A. Muller, T. B. Taylor, G. F. Smoot, F. von Hippel, H. Bethe, and W. K. H. Panofsky. 1975. "Report to the American Physical Society from the Study Group on Light-Water Reactor Safety." *Review of Modern Physics* 47 (Suppl. 1): S1–S123.

Mai, S., and C. Zimmerman. 2003. *Risk Analysis: Tool for Integrated Coastal Planning.* Proclamation of the 6th International Conference on Coastal and Port Engineering in Developing Countries, Columbo, Sri Lanka.

Mobus, C. 1979. "The Analysis of Non-Symmetric Similarity Judgments: Drift Model, Comparison Hypothesis, Tversky's Contrast Model and His Focus Hypothesis." *Archiv Fur Psychologie* 131 (2): 105–136.

Moore, D. R. J., B. E. Sample, G. W. Suter, B. R. Parkhurst, and T. R. Scott. 1999. "A Probabilistic Risk Assessment of the Effects of Methylmercury and PCBs on Mink and Kingfishers Along East Fork Poplar Creek, Oak Ridge, Tennessee, USA." *Environmental Toxicology and Chemistry*, 18 (12): 2941–53.

Ortwin, R. 1998. "Three Decades of Risk Research: Accomplishments and New Challenges." *Journal of Risk Research* 1 (1): 49–71.

Pate-Cornell, M. E., and P. S. Fischbeck. 1993. "Probabilistic Risk Analysis and Risk-Based Priority Scale for the Tiles of the Space Shuttle." *Reliability Engineering and System Safety* 40 (3): 221–38.

———. 1994. "Risk Management for the Tiles of the Space Shuttle." *Interfaces* 24 (1): 64–86.

Planning Research Corporation. 1989. *Independent Assessment of Shuttle Accident Scenario Probabilities for Galileo Mission and Comparison with NSTS Program Assessment.* Los Angeles: Planning Research Corporation.

Rasmussen, N. C. 1981. "The Application of Probabilistic Risk Assessment Techniques to Energy Technologies." *Annual Review of Energy* 6:123–38.

Rezmierski, V. E., D. M. Rothschild, A. S. Kazanis, and R. D. Rivas. *Final Report of the Computer Incident Factor Analysis and Categorization (CIFAC) Project.* Ann Arbor, MI: Regents of the University of Michigan. [Online report; retrieved 10/28/05]. http://www.educause.edu/ir/library/pdf/CSD4207.pdf.

Rogovin, M., and G. T. Frampton. 1980. *Three Mile Island: A Report to the Commissioners and to the Public.* Washington, DC: Government Printing Office.

Rotstein, A. H. 2002. "Shooting Leaves Four Dead at University of Arizona." *The Daily Texan:* World & Nation, October, 29.

Sadiq, R., T. Husain, B. Veitch, and N. Bose. 2003. "Distribution of Arsenic and Copper in Sediment Pore Water: An Ecological Risk Assessment Case Study for Offshore Drilling Waste Discharges." *Risk Analysis* 23 (6): 1309–21.

Safie, F. M. 1991. "A Statistical Approach for Risk Management of Space Shuttle Main Engine Components." In *Probabilistic Safety Assessment and Management: Proceedings of the International Conference on Probabilistic Safety Assessment and Management.* New York: Elsevier Science Publishing Co., Inc., 13–8.

———. 1992. "Use of Probabilistic Design Methods for NASA Applications." *American Society of Mechanical Engineers Symposium on Reliability Technology.* New York: American Society of Mechanical Engineers, 17–24.

———. 1994. "A Risk Assessment Methodology for the Space Shuttle External Tank Welds." *Annual Proceedings on Reliability and Maintainability Symposium.* Anaheim, CA: Reliability and Maintainability Symposium, 230–4.

Schmidt, S. R. 2004 "Autobiographical Memories for the September 11th Attacks: Reconstructive Errors and Emotional Impairment of Memory." *Memory and Cognition* 32 (3): 443–54.

Schwarz, G., and A. Tversky. 1980. "On the Reciprocity of Proximity Relations." *Journal of Mathematical Psychology* 22 (3): 157–75.

Science Applications International Corporation. 1995. *Probabilistic Risk Assessment of the Space Shuttle.* Washington DC: NASA.

Siegel, M. 2005. *False Alarm: The Truth About the Epidemic of Fear.* Hoboken, NJ: John Wiley and Sons.

Siegel, P. S., D. M. McCord, and A. R. Crawford. 1982. "An Experimental Note on Tversky's Features of Similarity." *Bulletin of Psychonomic Society* 19 (3): 141–2.

Slob, W., and M. N. Pieters. 1998. "A Probabilistic Approach for Deriving Acceptable Human Intake Limits and Human Health Risks for Toxicological Studies: General Framework" *Risk Analysis* 18 (6): 787–98.

Taylor, C., A. Krings, and J. Alves-Foss. 2002. "Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening." Paper presented at the ACM Workshop on Scientific Aspects of Cyber Terrorism, Washington, DC.

Tversky, A. 1977. "Features of Similarity." *Psychological Review* 84 (4): 327–52.

Union of Concerned Scientists. 1977. *The Risk of Nuclear Power Reactors: A Review of the NRC Reactor Study.* Cambridge, MA: Union of Concerned Scientists.

U.S. Nuclear Regulatory Commission. 1975. *Reactor Safety Study, WASH-1400.* Washington, DC: U.S. NRC.

———. 1983. *PRA Procedure Guide: A Guide to the Performance of Probabilistic Risk Assessments for Nuclear Power Plants, NUREG/CR-2300.* Washington, DC: U.S. Nuclear Regulatory Commission.

Voortman, H. G., P. van Gelder, and J. K. Vrijling. 2002. *Risk-Based Design of Large Scale Flood Defense Systems.* 28th International Conference on Coastal Engineering, Cardiff, Wales.