A Taxonomy for Analyzing Hazards to Information Systems

Richard Baskerville
Copenhagen Business School
Howitsvej 60
DK 2000 Frederiksberg, Denmark
Tel +45 3815 3763
Fax +45 3815 2401
Email dsrbask@hp2.cbs.dk

Abstract
Although information systems security is a serious problem, the nature of the constellation of hazards facing these systems is still not well understood. The existing taxonomies used to analyze hazards of three types: Asset groupings or impact groupings, and convenience groupings. Most of these taxonomies are problematic because they focus on consequences of the hazard, rather than on the nature of the hazard itself. This paper proposes a new taxonomy that analyzes deliberate and accidental hazards in different dimensions. The usefulness of the taxonomy is demonstrated by applying it to analyze a sample of hazard events. Its usefulness is further demonstrated by applying the taxonomy to a particular organizational setting.

Introduction: Distributing Security
The security of information systems is a serious problem. Compendiums of incidents of systems failures and abuses are widely available (*e.g.*, Parker 1976, Whiteside 1978, BloomBecker 1990, Hafner and Markoff 1991, Clough & Mungo 1992, Neumann, 1995). Textbooks and trade books discuss the potential solutions (*e.g.,* Martin 1973, Lane 1985, Baskerville 1988, Pfleeger 1989, Forcht 1994). Public agencies espouse national concerns about societal dependency on risky technologies (*e.g.*, CMND 8201 1981, National Research Council 1991, US Congress 1994).

Estimates of losses to computer abuse typically place the annual losses in billions. For example, Dixon *et al.* (1992) report a London Business School study that estimated 12 percent of computer-reliant companies were victims of fraud at an average loss of £46,000 (*ca.* $75,000). They also present an analysis of U.K. Audit Commission surveys that indicate a rise in the number of computer fraud incidents from 67 in 1981 to 118 in 1987 with the average loss per incident rising from £31,000 (*ca.* $50,000) in 1981 to £262,000 (*ca.* $425,000) in 1987. The French information technology security society (Clusif) reported a 15.5 percent increase in losses caused by security breaches in 1991 with a total estimated cost of 10.4 billion francs (*ca.* $2 billion) (Gannon, 1992). In the US, the annual costs of toll fraud alone is estimated to be over two billion dollars (Haugh *et al.* 1992).

For the purposes of this paper, we will use the term "hazard" to refer to a realized or potential event that would harm an information system. These hazards are also known by the terms "risk" or "threat". The term hazard is preferred over the term risk, because the concept of risk in some fields is synonymous with the concept of probability. The term threat connotes not only probability, but also intentionality which does not capture the essence of natural hazards. A hazard is generally defined as something that causes danger or peril. "Hazards" captures the idea of the essential source of any type of harm that might befall an information system.

We will also consider the concept of information systems security in its broadest sense. IS security and computer security are terms sometimes used narrowly to regard hazards intentionally posed by disgruntled workers, juvenile vandals, or industrial spies. In broad IS practice, however, these terms also regard unintentional hazards like errors and machine failure because the effects of the various protective measures impact both intentional and unintentional types of hazard.

This paper suggests that part of the difficulty of understanding the security problem lies in faulty models. Most of the current taxonomies of information systems hazards are problematic because they focus primarily on consequences of the hazard, rather than on the central nature of the hazard. Our purpose is to consider a new hazards taxonomy that may lead

to a better understanding of this problem and consequently lay the groundwork for a better understanding of the solutions.

Importantly for this conference, the rising use of distributed systems models is pushing many information systems management functions out into the organization. The systems management must necessarily become distributed along with the systems. Organizations have long depended on centralized security management. The attempt to centralize security in a distributed environment raises paradoxes that interfere with the benefits of distributed systems (Baskerville 1993). Some systems security functions must be distributed with the system. Our current lack of understanding about the nature of information system hazards will only serve to intensify the problems of distributed security. In the 21st century, we must provide the systems managers at all levels of the organization with clear, meaningful tools for analyzing their security hazards. The taxonomy proposed below is a definite advancement toward this goal.

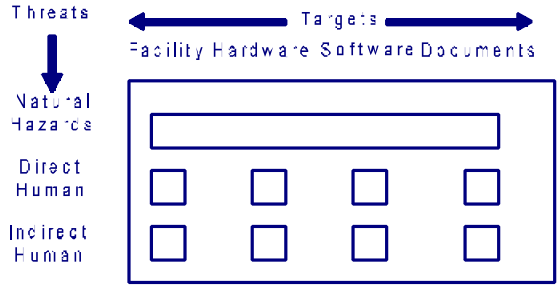

Figure 1. Smith-Lim asset grouping of hazards.

The paper is divided into five sections, including this introduction. Section two will analyze current taxonomies and discuss their shortcomings. The third section details the proposed hazard taxonomy. Section four demonstrates the usefulness of the taxonomy in helping us to understand the security problem. This demonstration consists of two applications of the new taxonomy: First, we use the taxonomy to investigate the proportions of a sample of hazard events. Second, we use the taxonomy to analyze a particular case. The final section suggests some implications and further research.

Taxonomies For The Analysis of Security Hazards

There are widely varied classification schemes proposed for analyzing information systems hazards in the security, audit and risk analysis literature. Most of these are closely associated with risk analysis or security management frameworks. These taxonomies are of three types: Asset groupings, impact groupings, and convenience groupings. Each of these is analyzed below:

Asset Groupings

Asset groupings use characteristics of IS assets as the primary criterion for dividing the spectrum of hazards into categories. For example, Smith-Lim (Smith and Lim 1985) primarily divide the hazards according to IS assets (or "targets"). These hazards fall into four categories: facility, hardware, software and documents. They use a second dimension taxonomy of three categories: natural hazards, direct human hazards and indirect human hazards. See Figure 1.

Parker (1981) uses a more complex taxonomy dividing hazards into five IS asset categories: data, application programs, systems programs, computer equipment and system service. Parker's analysis is mainly focussed on human error and tort and his second

SAFE Checklist Organization (844*)				Computer Security Handbook Checklist Organization (790)						AFIPS Checklist Organization (956)					
	M	DE	DI		M	DE	DI	T	DN		M	DE	DI	T	DN
1. Personnel Practices, (66)	2	2	2	1. Management Risk & Security, (25)	4	4	4	4	4	1. Natural Disasters (10)	3	3	3	3	3
2. Physical Security, (161)	4	4	4	2. Employees, (24)	2	2	2	2	2	2. Criminal Acts (40)	4	4	4	4	4
3. Operating Procedures, (76)	5	5	5	3. Legal Issues, (17)	5	5	5	5	5	3. Operating Integrity (184)	5	5	5	5	5
4. Backup and Contingency Planning, (63)	1	5	5	4. Computer Crime, (82)	5	5	5	5	5	4. Backup and Recovery, (85)	1	1	1	1	1
5. Systems Development and Maintenance, (54)	3	3	3	5. Contingency Planning, (20)	3	3	3	3	3	5. Administrative Controls, (130)	1	1	1	1	1
6. Data Base Security, (101)	5	5	5	6. Risks and Insurance, (16)	2	2	2	2	2	6. Systems Hardware and Software, (83)	5	5	5	5	5
7. Data Communications Security, (114)	5	5	5	7. Auditing, (95)	5	5	5	5	5	7. Communications, (118)	5	5	5	5	5
8. Systems and Access Control Software, (89)	1	1	1	8. Application Controls, (101)	5	5	5	5	5	8. Distributed Risk, (102)	1	1	1	1	1
9. Insurance, (17)	1	1	1	9. Hardware Security, (55)	5	5	5	5	5	9. Applications, (156)	1	1	1	1	1
10. Security Planning and Administration, (45)	1	1	1	10. Facility Security, (32)	5	5	5	5	5	10. The Security Audit, (51)	1	1	1	1	1
11. Application Controls, (58)	5	5	5	11. Monitoring and Control, (53)	5	5	5	5	5						
				12. Software and Data, (16)	5	5	5	5	5						
				13. Data Files, (52)	5	5	5	5	5						
				14. Encryption, (7)	5	5	5	5	5						
				15. Communications Networks, (26)	5	5	5	5	5						
				16. Forms and Supplies, (82)	5	5	5	5	5						
				17. Contract Services, (50)	5	5	5	5	5						
				18. Mini and Microcomputers, (27)	5	5	5	5	5						

Acts Codes
M - Modification
DE - Destruction
DI - Disclosure
T - Taking
DN - Denial of use

Exposure Scale
blank 1
2 up to 20%
3 up to 40%
4 up to 60%
5 up to 80%
up to 100%

*The number of items in each checklist is noted after each list name.

Figure 4. Comparative checklist risk categories illustrating convenience groupings.

Figure 3. Courtney's impact grouping of hazards.

Figure 5. Forscht's taxonomy of computer risks.

Figure 2. Parker's asset group of hazards.

dimension is confined to the roles of various people in computer systems. See Figure 2.

A major shortcoming of asset groupings for analyzing hazards is that the taxonomy fails severely to meet the standard of mutual exclusivity. In other words, a single hazard can affect several, if not all categories of asset. For example, a coffee cup spilled into a disk unit might destroy both equipment and data. Asset groupings also lack completeness. For example, it is not clear how hazards to privacy would be analyzed using this taxonomy.

Impact Groupings

Impact groupings are the very widely known taxonomies for classifying IS hazards. The impact of a hazard is specified without concern for the exact assets underlying the loss. Courtney (1977) classified hazards primarily in three categories: disclosure, modification, and destruction. As a second dimension, he distinguished hazards by two possible motives: intentional and accidental. A variation appeared in the widely known FIPS Pub 65 (U.S. National Bureau of Statistics, 1979), with three different titles for the same three primary concepts: Data confidentiality, data integrity, and processing availability. (See Figure 3).

This taxonomy suffers from the same problem of mutual exclusivity. Using the earlier example, the spilled coffee would destroy the disk, but the secondary impact is modified data if slightly out-of-date backup tapes are used to restore the new disk. The consequences of a single hazard may snake through the entire impact taxonomy. This scheme also lacks completeness in a different dimension, for example it is not clear how software piracy would be classified in this taxonomy.

Convenience Groupings

Some widely published taxonomies disregard analytic criteria altogether, using categories that lack parallelism as well as mutual exclusivity. These taxonomies seek completeness without deep concern for the order in the categories, juxtaposing seemingly unrelated issues as parallel

Neumann's Taxonomies			
1. Problem Sources	2. Reliability and Safety	3. Misuse Technique Classes	4. Security and Integrity Problems
Requirements Definition System design HW implementation SW implementation System operation Misuse HW malfunction Environment Analysis Maintenance	Communication systems Space Defense Aviation Trains Ships Control systems Robotics Medical systems Power systems Computer clocks Computer errors	External misuse Hardware misuse Masquerading Pest programs Controls bypass Active misuse Passive misuse Misuse by inaction	Intentional misuse Security accidents Spoofs and pranks Intentional denials of service Unintentional denials of service Financial fraud by computer Accidental financial losses Risks in elections Jail security Privacy

Figure 6. Neumann's analysis of computer related risks.

categories (*e.g.*, "Hardware Security" versus "Forms and Supplies"). Typically, these taxonomies are used as organizing mechanisms for design or audit checklists. While the groupings are tidy, the categories themselves were never intended as an analytical tool for the discovery of hazards. Figure 4 is a comparison between the high-level categories of three major checklists. Notice that these taxonomies mix such varied categories as assets in need of protection, organizational policies, and technical safeguards. Another example can be found in Forcht (1994), who uses the organization in Figure 5 when discussing threats to computer security. While these categories serve to raise a broad range of issues regarding hazards, they jumble hazards and safeguards together.

Discussion

All of the taxonomies above are problematic because they focus on consequences of the hazard, rather than on the nature of the hazard. Asset-based taxonomies are concerned with the organizational components that need protection. Impact-based taxonomies are tightly focussed on the results of the hazards' occurrence. Convenience taxonomies are more detailed and complete, but lack structures to help security novices understand any unspecified potential hazards.

Neumann's Analysis

Neumann (1995) presents a meticulous analysis of information systems hazards based on ten years of moderation of the on-line computer newsgroup *Forum on Risks to the Public in the Use of Computers and Related Systems*. The issues are analyzed from many perspectives and use several independent taxonomies. The primary taxonomies are sources of development problems, reliability and safety, misuse technique, and security and integrity problems. The major categories in these taxonomies are shown in Figure 6.

Neumann's analysis is centric on taxonomy of problem sources that reflects an extended life cycle view of information systems (shown in column 1 of Figure 6). Some in the auditing community also favor such a viewpoint (*cf.* Gallegos, Richardson and Borthick 1987). The view can be thought of as extended because there are separate categories for misuse, malfunction and environment. These categories help deepen the analysis of the traditional operational stage of the system life cycle. This life cycle analysis is particularly useful to call attention to the depth (in a general systems sense) from which human errors can spring to create hazards in information systems.

Neumann distinguishes two major classes of hazards: (1) reliability and safety, and (2) security. These classes equate roughly to (1) accidental and (2) intentional hazards. Neumann provides separate taxonomies for analyzing each of these two major classes (shown in columns 2 and 3 of Figure 6). The reliability and safety taxonomy, although somewhat similar to an impact grouping, is a useful tool for educating systems managers about the hazards particular to an industry group. At the same time, the breadth of the categories demonstrate the universal nature of the general security problem. The security taxonomy is derived from earlier work on misuse techniques. Neumann analyzes each category in these two taxonomies using the central problem sources model (the life-cycle based taxonomy in column 1) as an underlying second dimension.

Despite the careful distinctions made between the two major classes of hazard, Neumann argues in favor of a common framework for considering reliability problems and security problems:

Problems that are seemingly completely unrelated to security may nevertheless have security implications. . . . A system cannot be secure unless it is adequately reliable, and cannot be either reliable or available if it is not adequately secure. (p. 131)

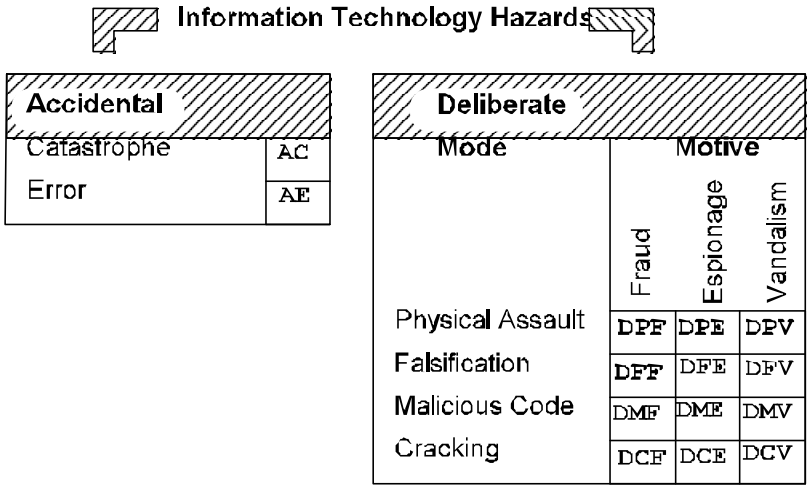

Figure 7. Information Systems Hazards

The common framework is the taxonomy of security and integrity problems, shown in column 4 of Figure 6. These categories are also analyzed in terms of the central problem sources model (the life cycle-based taxonomy in column 1).

Neumann's work represents a major advancement in the study of these hazards. Still, several problems remain. For example, using a life cycle model as centric is a narrow view. Life cycle models are only one of several systems development models. Development modes commonly found in distributed environments, such as prototyping and end-user computing are not well considered in this model. Another problem is that the final taxonomy of security and integrity problems lacks parallel criteria for the analysis. Despite the meticulous preparation, the common framework appears as a convenience grouping. It arrives as an independent analysis, and it is not shown how it proceeds from the analysis of the two major classes of hazards. This makes the common framework more difficult for unindoctrinated system managers (such as those in distributed environments) to apprehend the analysis. Consequently, it becomes much more difficult for distributed practitioners to adapt this taxonomy to widely-varied field settings and system development models.

Hazard Taxonomy

This paper describes a taxonomy of hazard which offers improved parallelism, mutual exclusivity and completeness. More importantly, this taxonomy is based on the nature of the hazards themselves, not on its impact or the assets it might damage.

Overview of Hazards Taxonomy

We will also develop a framework for considering various hazards according to certain distinguishing characteristics. The accidental-deliberate dimension remains as the high-level distinguishing characteristic that primarily divides hazards into two classes (See Figure 7). However, beyond this fairly familiar dichotomy, we will not attempt to maintain a symmetrical analysis of the two types. Accidental and intentional hazards fundamentally differ in their characteristic dimensionality, as we will demonstrate later in this section.

Accidental hazards can be usefully analyzed using a simple two-class, one-dimensional taxonomy. Accidental hazards arise as either errors or catastrophes. Attempts to further classify these categories typically break down over ambiguities. For example, we attempted to distinguish human errors, design errors and machine error. This is difficult with computers because most errors described as "computer error" can indeed be traced to an operator or

programmer error. Many operator and programmer errors can be further traced to problems with software designs. It is less problematic to distinguish between "errors" as a whole (typically human mistakes), from "catastrophes" or acts-of-nature that are clearly not human artifacts.

Deliberate hazards arise intentionally from the people who interact with information systems and IS development. Unlike accidental hazards, deliberate hazards are most usefully analyzed with a multiple-category, two dimensional taxonomy. Deliberate hazards can be classified according to the person's basic approach (or "mode") to creating the hazard. These approaches range from physical break-ins of computer facilities to logical cracking of operating systems via telecommunications. Once classified by approach, however, these hazard categories all share characteristics regarding the person's primary motivation for posing such hazards. The primary reasons people attack information technology are for the purposes of fraud, espionage or vandalism.

Accidental Hazards

The distinguishing characteristic of accidental hazards is that these hazards are not intentionally posed by humans. The term "catastrophe" refers to natural types of hazards that involve a sudden or violent disturbance leading to a disastrous end and are more-or-less a natural consequence of depending on computer-based systems. This definition of catastrophe includes those events legally defined as "acts of God." An act of God is a natural force operating without human agency such as flood, lightning, earthquake and tornado. It is useful to broaden the concept of accidental catastrophe, however, to include mechanical or electrical component failures, accidental fires, collisions, spillage, *etc*.

We can further classify accidental catastrophes as mechanical or electrical component failure and as natural disasters and weather storms. An example of the former is a fuse that blew in a main Ohio Bell telephone switch computer that disrupted 54,000 telephone lines and related services in Worthington, Ohio for 24 hours (Neumann 1993a). Another example was a burst pipe that poured fifty gallons of water through the ceiling of the Wycombe General Hospital computer facility and into the memory unit of their mainframe taking out the patient administration system for six hours ("Rain sickens" 1992). An example of a natural disaster was a heavy snow build up on the roof of a computer center in Clifton, New Jersey that caused the roof to collapse. The loss of this data center brought down a network of 5000 Automatic Teller Machines across the United States (Neumann 1993b)

Modes of Deliberate Hazards

There five distinct modes or approaches that people may take when intentionally creating hazards for information systems:

FALSIFICATION hazards regards using computer technology to create untrue data or to counterfeit or forge computer-based information. This includes altering or adding to data in such a way to make the resulting information a misrepresentation. That is, people can pose hazards for computer-based systems by simply feeding false input into the systems. Well designed systems are less vulnerable to such falsification, however, the automated nature of computer processing will often allow unusual transactions to go unnoticed for long periods of time. For example, three Michigan banks lost $200,000 in a scheme that involved 30 conspirators. ATMs were used to deposit worthless checks, which were automatically credited. The funds were then withdrawn from ATMs before the checks bounced (Bray 1993).

PHYSICAL ASSAULT hazards includes threats or attempts to inflict tangible damage on computing or telecommunications machinery, media, furniture, personnel or related rooms, buildings, and support apparatus. It also includes physical attacks on computer-related installations such as trespassing, wiretapping, breaking-and-entering, and impostering. It is not always necessary for a person to employ highly sophisticated technology in posing a hazard for a computer system. If the physical security is lax enough, people may be able to walk through an unlocked door, switch on a terminal, and press a function key that automatically logs into a computer system. Such physical assaults are often unsophisticated, straight-forward, very easy and, too frequently, very effective.

Physical assaults include scavenging through organizational rubbish in search of confidential printouts, user id and password notes, or program documentation. Physical

assaults also include telephone spoofing, in which users or system professionals are tricked into giving out confidential information over the telephone. Types of physical assault include intrusion, eavesdropping, wiretapping and passive interception. An example of physical assault is a burglary of the computer room in a London branch of Barclays International. The burglars were not after cash, but software that would allow them to break into a global electronic funds transfer banking network (Evans 1991).

CRACKING entails a logical break-in into computer systems or software by guessing or decrypting access codes, account names, passwords and files. Crackers often have strong technical knowledge, and approach systems by electronically "browsing" communication networks and computer assets. Cracking activities are often associated with software piracy and phone phreaking. Software piracy sometimes involves breaking copy protection schemes. Phone phreaking involves various schemes for defeating telephone or computer network billing and control systems in order to obtain "free" communications and services. An example is the penetration of the Prestel system by a group of crackers using 2222222222 as the user id and 1234 as the password. Their frolic through the system included sending email from the account of HRH the Duke of Edinburgh and changing exchange rates on the *Financial Times* pages (Clough and Mungo 1992). Another example is the famous case of the German hackers who easily broke into U.S. government computers all over the world in an attempt to extract valuable information for sale to spies (Stoll 1989).

MALICIOUS CODE regards programs that divert computing resources, alter data, or expose sensitive information to unauthorized people. The programs often run undetected by the other computer users, making malicious code a sinister way of enlisting the computer to aid in its undoing. Examples of malicious code include logic bombs, Trojan Horses, viruses, worms, trap doors, salami routines and spoof programs. The classic example is the Morris worm, which broke down much of the internet, and choked thousands of computers by exploiting known bugs in the Unix operating system (Hafner and Markoff 1991).

Motives for Deliberate Hazards
There are three distinct motives for deliberate hazards:

FRAUD regards a deliberate deception for the purposes of unfair or unlawful gain. Fraud is perhaps the most basic type of computer crime. Legally, there are two types of fraud, actual and constructive, determined partially by intent. Actual frauds involve intentional criminal deception to cheat someone. Constructive frauds do not require malicious intent, but occur when someone is misled into parting with something of value. The majority of all valuable commodities (*e.g.*, money, precious metals, inventories) are accounted through electronic computers. The ownership of much of the earth's fortunes are essentially represented in computer storage devices and memories. These fortunes are processed, manipulated and exchanged through computer programs. There are many ways in which computers can be used to misappropriate such fortunes. Frauds can be sub-categorized as theft of recorded funds, theft of data, intentional data corruption, theft of programs, theft of computing resources, theft of communications, and computer-aided fraud. For example, an authorized user misused his legitimate access to hack a British local authority's computerized housing finance system. He transferred £67,000 to a phony building society (savings and loan) account by generating checks to a legitimate contractor for illegitimate contracts. He was caught because the building society became suspicious about his large withdrawals from the phony account ("Man hacks" 1992).

ESPIONAGE is the practice of spying to obtain otherwise private information. Typically it involves three steps: gaining access to private data, capturing the data, and analyzing the data. The ultimate outcome of the espionage process is to inevitably reduce the information value of the data. This outcome results because the stolen data had typically been kept private because of its value. When publicized or shared with a competitor, the information value of the data is reduced. People involved in espionage may act as intruders, plants, or recruits. Typically, computer system espionage involves unauthorized access to the data in an organization's computer system. An example of this class of hazards include a British Telecom employee in their debt-control department who repeatedly requested (and was denied repeatedly) access

the company data bank in his pursuit of unpaid debts to BT. He eventually hacked his way into the data bank anyway and recovered over £200,000 in bad debts. Although BT tried to dismiss him for misconduct, an industrial tribunal ordered his reinstatement ("Hack-happy BT" 1992)

VANDALISM regards willful or malicious destruction of computer resources including machinery, data and software. The term is used very broadly to include acts of vandalism by individuals or groups, and encompasses such types as juvenile mischief, individual vengeance, public disorder, terrorism and warfare. As an example, an unknown hacker broke into an Italian newspaper computer on several occasions. The computer was used by the editorial staff to prepare copy for publication. Advertisements, crossword puzzles and horoscopes were altered into obscene, offensive phrases. Some changes were caught, others were published. (Neumann 1992)

Computer warfare is a type of vandalism that is of growing interest. Military information systems are highly subject to subversion and destruction as military targets, and are subject to "hardening" to reduce vulnerability. This hardening concept is being extended to civilian systems on which the military also depends, for example, those involved in the planning, design and production of war materials (Madsen 1992).

Applying The Taxonomy

This model provides a vehicle that opens a new viewpoint from which to understand the information systems security problem. The practical implications of this new viewpoint can be understood by examining the information security problem in a community sense using the model. We can consider this by examining a collection of published security vignettes and classifying the hazards according to the model. The model may also be useful in studying unique organizational security settings. We will also consider this by examining such a case with this model.

Published Vignettes

Quantification of the hazards of information systems security is known to be problematic, but two issues rise to the fore. First, many professionals believe that the under-reporting of computer crime inevitably skews descriptive statistics in the security arena. The under-reporting undoubtedly exists; such recognized authorities as Donn Parker (Parker 1976) and Robert Courtney (Courtney 1986) refer to it. The extent of the variance between actual computer abuse and reported computer abuse is known as the "dark figure," estimated between six and one hundred times larger than reported abuse. The second issue concerns the ambiguous definitions of "computer" abuse. The characteristics that distinguish computer abuse from other types of white-collar crime are very fuzzy, especially as the computer has become ubiquitous in management. Although both issues focus on criminal losses, there are relevant parallels in accidental losses (*e.g.*, institutional embarrassment over such professional negligence as inadequate backups).

Accepting the caveat that such quantitative analyses have limited validity, we can still demonstrate how the model discussed here can help us understand hazards to information systems in a global sense. The model was used to analyze the vignettes published in the "Risks to the Public" column edited by Peter G. Neumann in *Software Engineering Notes* for two years (January, 1992, 17:1 through October, 1993, 18:4). This column lists computer-related risks and hazards reported to the newsletter (through the internet newsgroup mentioned earlier) by various interested parties. This data is very much a convenience sample, but based on critiques of existing quantitative studies, it is probably no less of a legitimate sample than those underlying most published descriptive statistics. Each information systems hazard reported in this column was classified according the model. During this two-year period the column cited reports of 147 distinct incidents of hazards that damaged organizations and appeared to arise from the use of computer-based systems.

	Hazards Analysis							
Accidental	n	%						
Catastrophe	17	19.1%						
Error	72	80.9%		49.0%	of total			
Total	89	60.5%						
Deliberate	Fraud		Espion		Vandal		Total	
	n	%	n	%	n	%	n	%
Physical	3	5.2%	0	0.0%	0	0.0%	3	5.2%
False	14	24.1%	5	8.6%	0	0.0%	19	32.8%
Malicious	3	5.2%	1	1.7%	8	13.8%	12	20.7%
Cracking	9	15.5%	2	3.4%	13	22.4%	24	41.4%
Total	29	50.0%	8	13.8%	21	36.2%	58	100.0%
Total Hazards	147							

Figure 8. Analysis of hazards vignettes.

Figure 8 is a simple descriptive table of this analysis. From this we learn a little about the relationship between deliberately caused computer hazards and the two types of accidental hazards. Deliberate hazards account for only forty percent (58) of the events. Sixty percent of the hazards were accidental. Of these accidental events, more than three-quarters were caused by errors. As a matter of fact, just under half of all reported hazards were the result of errors. Seventeen percent of the accidental hazards were related to a catastrophe.

If we study the population of deliberate hazards according to the motive dimension, we find that the largest group, half of deliberate hazards (50%), was classified as fraud-motivated. Approximately 36% of these hazards were motivated by vandalism. The remaining hazards (14%) were attributed to espionage. Similarly, the frequency of each mode of deliberate hazard is analyzed. More than a third of the events (41%) primarily involved cracking, another third (33%) involved falsified system data, 21% were attributed to malicious code, and three incidents regarded physically exploited system resources.

If we used this analysis as a means of setting priorities for attending to information systems hazards, we should focus on improving systems immunity to the following types of hazards:

Errors ..... 49% of total events
Catastrophes ..... 12% of total events
Fraud by falsification ..... 10% of total events
Vandalism by cracking ..... 9% of total events

These four categories accounted for 80% of the events in the sample. If we add fraud by cracking (6%) and vandalism by malicious code (5%), we account for 91% of the events. This demonstrates how useful the model can be for setting priorities for the development of improved safeguards for information systems.

Telephone Company Case Study

Some authorities on risk analysis have promoted the use of a "due care" concept as a criterion for determining the appropriate set of safeguards in an information system (Parker 1986) Another application for this taxonomy would be its use as one tool to help insure that the hazard analysis is thorough. Assurance of such a thorough analysis represents one step in the process of satisfying this due care criterion for establishing a reasonable set of security safeguards in an information system.

To illustrate the potential of this taxonomy, a regional telephone utility in the Northeastern US used the taxonomy to analyze the spectrum of information system hazards confronting its small data center. The examples below are examples of the hazards that the organization was able to classify using the model.

- Accidental Catastrophe: Faulty diskettes
- Deliberate Physical Assault (Fraud): Changing modem configurations to allow auto-answer for remote dial-up
- Deliberate Physical Assault (Espionage): Obtaining proprietary blue prints or sketches
- Deliberate Physical Assault (Vandalism): Tampering with off-site backup storage tapes
- Falsification (Fraud): Modify toll dates to try and get credit
- Deliberate Falsification (Espionage): Stealing non-published telephone information
- Deliberate Falsification (Vandalism): Modify or delete any operating system files
- Deliberate Malicious Code (Fraud): Low quality software programs
- Deliberate Malicious Code (Espionage): Intercept transfer of data over telephone lines
- Deliberate Malicious Code (Vandalism): Corrupt firmware in hardware products
- Deliberate Cracking (Fraud): Stealing access codes for telephone credit cards
- Deliberate Cracking (Espionage): Using telephone knowledge and services to rig telephone call in contests
- Deliberate Cracking (Vandalism): Break-in for the purpose of deleting objects through dial-up causing system reconfiguration.

Discussion

These two applications of the taxonomy show that it can improve our understanding of information systems hazards at two levels of abstraction. At one level, the taxonomy is useful in studying particular instances of information systems security. The taxonomy can be used to structure a search through the constellation of possible hazards in order to exercise due care in discovering the necessary set of system safeguards. At a second level, the taxonomy is useful in studying the general patterns of hazards to information technology in order to understand the status or trends in these hazards.

Implications and Further Research

The practical implications of this taxonomy also lie in these two levels of abstraction. A better understanding of the status and trends of information systems hazards will help us to develop devices, procedures and training to direct protective resources toward the major risk areas. The use of the same taxonomy in particular analyses will lead those responsible for systems reliability to place appropriate safeguards for their systems. The effect of the due care criterion will improve these systems. This will enable these professionals to more quickly and appropriately take advantage of those devices and techniques discovered at the community level.

The research needs also align with these two levels of abstraction. At the community level, we need to confirm the proportions of risk suggested by the taxonomy with more thorough empirical work. This might involve analyzing the commercial risk analysis threat databases according to the model, or collecting data directly from organizations regarding threat occurrences in a recent period. At the particular level, we need to develop heuristics for translating the hazard analysis into safeguards. This would likely involve using this same

taxonomy as a classification system for safeguards that are particularly effective against specific classes of threats. In turn, this implies that we need to study the effects of particular safeguards as protective measures against each of the hazard classes in the taxonomy.

References

Baskerville, R. 1988. *Designing Information Systems Security*. Chichester: J. Wiley.

Baskerville, R. 1993. Information systems security: Adapting to survive. *Information Systems Security 2* (1) (Spring), pp. 40-47.

BloomBecker, B. 1990. *Spectacular Computer Crimes: What They Are And How They Cost American Business Half A Billion Dollars A Year*. Homewood, Illinois: Dow Jones-Irwin.

Bray, Hiawatha. 1993. 30 indicted in ATM scheme. *Free Press* (24 April).

Clough, B. and Mungo, P. 1992. *Approaching Zero: Data Crime and the Computer Underworld*, London: Faber and Faber.

CMND 8210. 1981. 1981 census of population: confidentiality and computing. London: HMSO, March.

Courtney, R. 1977. Security risk assessment in electronic data processing. *AFIPS Conference Proceedings NCC* 46, pp. 97-104.

Courtney, R. 1986. The state of the art in data security. *Thirteenth Annual Computer Security Conference*. Computer Security Institute, Atlanta, November, pp. RC3-RC33.

Dixon, R., Marston, C. & Collier, P. 1992. A report on the joint CIMA and IIA computer fraud survey, *Computers & Security 11*, 4 (July), 307-313.

Evans, Joanne 1991 SWIFT banking network targeted in London raid. *Computing*. (31 October) p.2.

Forcht, K.A. 1994. *Computer Security Management*, Danvers, Massachusetts: Boyd & Fraser.

Gallegos, F.; Richardson, D. and Borthick, A. 1987. *Audit and Control of Information Systems*. Cincinnati: South-Western.

Gannon, P. 1992. French losses rise sharply. *Computer Fraud and Security Bulletin*. (October) p.3.

Hack-happy BT debt chaser puts job on the line. 1992. *Computing* (9 July) p.1.

Hafner, K. and Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on The Computer Frontier*. New York: Simon & Schuster.

Haugh, J., Burney, R., Dean, G. and Tich, L. 1992. *Toll Fraud and Telabuse: A Multibillion Dollar National Problem.* Portland Oregon: Telecommunications Advisors.

Lane, V.P. 1985. *Security of Computer Based Information Systems*. London: Macmillan.

Madsen, Wayne. 1992. Government-sponsored computer warfare and sabotage. *Computers & Security 11* 3 (May), pp. 233-236.

Man hacks into council system to pay debts. 1992. *Computing* (6 August) p.2.

Martin, J. 1973. *Security, Accuracy and Privacy in Computer Systems*. Englewood Cliffs: Prentice Hall.

National Research Council. 1991. *Computers At Risk: Safe Computing in The Information Age.* Computer Science and Telecommunications Board, System Security Study Committee. Washington: National Academy Press.

Neumann, P.G. (ed) 1992. Risks to the public in computers and related systems. *Software Engineering Notes 17* (1), p.6).

Neumann, P.G. (ed) 1993a. Risks to the public in computers and related systems. *Software Engineering Notes 18* (2), p.12.

Neumann, P.G. (ed) 1993b. Risks to the public in computers and related systems. *Software Engineering Notes 18* (3), p.4.

Neumann, Peter G. 1995. *Computer Related Risks*. New York: ACM Press.

Parker, D. 1976. *Crime by Computer*. New York: Chas Scribners Sons.

Parker, D. 1981 *Computer Security Management*. Reston: Reston.

Parker, D. 1986. *Computer Crime: Computer Security Techniques,* US Department of Justice Bureau of Justice Statistics Document J29.2:C86.

Pfleeger, C. 1989. *Security in Computing*. Englewood Cliffs: Prentice-Hall.

Rain sickens data center. 1992. *Computing* (30 April). p.1

Smith, S. and Lim, J. 1985. Risk analysis in computer systems--An automated procedure. *Information Age 7* (1) (January) pp. 15-18.

Stoll, C. 1989. *The Cuckoo's Egg: Tracking A Spy Through The Maze of Computer Espionage.* New York: Doubleday.
U. S. National Bureau of Standards. 1979. Guideline for Automatic Data Processing Risk Analysis. Federal Information Processing Standards Publication FIPS 65, August.
U.S. Congress, Office of Technology Assessment. 1994. *Information Security and Privacy in Network Environments.* OTA-TCT-606. Washington, D.C.: U.S. Government Printing Office (September).
Whiteside, T. 1978. *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. Toronto: Fitzhenry and Whiteside.

1. Parker, D. 1976. *Crime by Computer*. New York: Chas Scribners Sons.

2. Whiteside, T. 1978. *Computer Capers: Tales of Electronic Thievery, Embezzlement, and Fraud*. Toronto: Fitzhenry and Whiteside.

3. BloomBecker, B. 1990. *Spectacular Computer Crimes: What They Are And How They Cost American Business Half A Billion Dollars A Year*. Homewood, Illinois: Dow Jones-Irwin.

4. Hafner, K. and Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on The Computer Frontier*. New York: Simon & Schuster.

5. Clough, B. and Mungo, P. 1992. *Approaching Zero: Data Crime and the Computer Underworld*, London: Faber and Faber.

6. Neumann, Peter G. 1995. *Computer Related Risks*. New York: ACM Press.

7. Martin, J. 1973. *Security, Accuracy and Privacy in Computer Systems*. Englewood Cliffs: Prentice Hall.

8. Lane, V.P. 1985. *Security of Computer Based Information Systems*. London: Macmillan.

9. Baskerville, R. 1988. *Designing Information Systems Security*. Chichester: J. Wiley.

10. Pfleeger, C. 1989. *Security in Computing*. Englewood Cliffs: Prentice-Hall.

11. Forcht, K.A. 1994. *Computer Security Management*, Danvers, Massachusetts: Boyd & Fraser.

12. CMND 8210. 1981. 1981 census of population: confidentiality and computing. London: HMSO, March.

13. National Research Council. 1991. *Computers At Risk: Safe Computing in The Information Age.* Computer Science and Telecommunications Board, System Security Study Committee. Washington: National Academy Press.

14. U.S. Congress, Office of Technology Assessment. 1994. *Information Security and Privacy in Network Environments.* OTA-TCT-606. Washington, D.C.: U.S. Government Printing Office (September).

15. Dixon, R., Marston, C. & Collier, P. 1992. A report on the joint CIMA and IIA computer fraud survey, *Computers & Security 11*, 4 (July), 307-313.

16. Gannon, P. 1992. French losses rise sharply. *Computer Fraud and Security Bulletin*. (October) p.3.

17. Haugh, J., Burney, R., Dean, G. and Tich, L. 1992. *Toll Fraud and Telabuse: A Multibillion Dollar National Problem*. Portland Oregon: Telecommunications Advisors.

18. Baskerville, R. 1993. Information systems security: Adapting to survive. *Information Systems Security 2* (1) (Spring), pp. 40-47.

19. Smith, S. and Lim, J. 1985. Risk analysis in computer systems--An automated procedure. *Information Age 7* (1) (January) pp. 15-18.

20. Parker, D. 1981 *Computer Security Management*. Reston: Reston.

21. Courtney, R. 1977. Security risk assessment in electronic data processing. *AFIPS Conference Proceedings NCC* 46, pp. 97-104.

22. U. S. National Bureau of Standards. 1979. Guideline for Automatic Data Processing Risk Analysis. Federal Information Processing Standards Publication FIPS 65, August.

23. Forcht, K.A. 1994. *Computer Security Management*, Danvers, Massachusetts: Boyd & Fraser.

24. Neumann, Peter G. 1995. *Computer Related Risks*. New York: ACM Press.

25. Gallegos, F.; Richardson, D. and Borthick, A. 1987. *Audit and Control of Information Systems*. Cincinnati: South-Western.

26. Neumann, P.G. (ed). 1993a. Risks to the public in computers and related systems. *Software Engineering Notes 18* (2), p.12.

27. Rain sickens data center. 1992. *Computing* (30 April). p.1

28. Neumann, P.G. (ed) 1993b. Risks to the public in computers and related systems. *Software Engineering Notes 18* (3), p.4.

29. Bray, Hiawatha. 1993. 30 indicted in ATM scheme. *Free Press* (24 April).

30. Evans, Joanne 1991 SWIFT banking network targeted in London raid. *Computing*. (31 October) p.2.

31. Clough, B. and Mungo, P. 1992. *Approaching Zero: Data Crime and the Computer Underworld*, London: Faber and Faber.

32. Stoll, C. 1989. *The Cuckoo's Egg: Tracking A Spy Through The Maze of Computer Espionage.* New York: Doubleday.

33. Hafner, K. and Markoff, J. 1991. *Cyberpunk: Outlaws and Hackers on The Computer Frontier*. New York: Simon & Schuster.

34. Man hacks into council system to pay debts. 1992. *Computing* (6 August) p.2.

35. Hack-happy BT debt chaser puts job on the line. 1992. *Computing* (9 July) p.1.

36. Neumann, P.G. (ed) 1992. Risks to the public in computers and related systems. *Software Engineering Notes 17* (1), p.6).

37. Madsen, Wayne. 1992. Government-sponsored computer warfare and sabotage. *Computers & Security 11* 3 (May), pp. 233-236.

38. Parker, D. 1976. *Crime by Computer*. New York: Chas Scribners Sons.

39. Courtney, R. 1986. The state of the art in data security. *Thirteenth Annual Computer Security Conference*. Computer Security Institute, Atlanta, November, pp. RC3-RC33.

40. Parker, D. 1986. *Computer Crime: Computer Security Techniques,* US Department of Justice Bureau of Justice Statistics Document J29.2:C86.