Risk Management from a Technological Perspective

by Vernon Leslie Grose, D. Sc.*

1. Introduction

Risk Management – as a term and concept – was coined initially in insurance circles. Its definition, scope, and application have proliferated over the past three decades until Risk Management now consists of a fairly diverse “spectrum” of management concepts to minimize loss. It is a very lopsided spectrum, however – dominated on one end by the insurance industry that spawned it.

The opposite – and more recent – end of the Risk Management spectrum could be described as *technological* instead of *financial*. It is from that end that I became interested and involved in managing risk.

2. Universal moral underpinning?

Perhaps everyone who enters the field of Risk Management is initially drawn to it by a *moral motivation* – whether to reduce dollar loss via sound loss financing, preclude disaster by forethought and preparation, or protect legitimate gains against capricious destruction. My entry, though provoked by moral outrage, differs from many others in the field.

In the mid-1950's, I was an applied physicist at Boeing working on the BOMARC ground-to-air guided missile. It was a very unreliable weapon system – so much so that all Air Force performance specifications; e. g. “the missile must launch and intercept an incoming enemy aircraft 80% of the time”, were renegotiated by Boeing to *half* those values. But even those pitifully low percentages could not be met by the missile! Tax-payers were paying for junk – but unknowingly because BOMARC was a secret project.

Why was this charade going on? Was it due to impossible technological barriers or insolvable problems? No. There was simply an unreasonable focus on *benefit over risk*, an unwillingness to identify and evaluate hazards in an evenhanded manner (Cost-Plus-Fixed-Fee contracts provide profit for “fixing mistakes” so *preventing* risks is a disincentive!), and a needlessly rushed mindset that believed that “we can always go back and fix any problems that may develop”. This situation so provoked my conscience that I became a crusader for truth, accuracy, and integrity in weapon development.

* Chairman, OMEGA SYSTEMS GROUP, Arlington, Virginia.

3. Reliability as Risk Management precursor

By 1956, those sharing my concern had initiated a technical management discipline known in the aerospace industry as *Reliability*, and I became an early contributor. My interest in Reliability continued as I began working in America's manned space program. However, something very unfortunate had happened to Reliability by the early 1960's – it was captured by “numerologists” who twisted and misapplied statistics in an attempt to describe everything by numbers. This entrancement with probabilities forced the abandonment of any concern about human behavior and focused instead exclusively on *equipment*, resulting in only a partial picture of reality.

4. Rise and fall of System Safety

To recapture the holism abandoned by Reliability numerologists, a new discipline arose – *System Safety*. It was about 4 years old in 1967 when it received a major boost in management recognition from the Apollo 204 fire that killed three astronauts. Our space program differed from defense programs in at least two major ways. First, it had no security classification and thereby was exposed to the public via news media. Failures could not be hidden as easily. Second, Wernher von Braun – who appointed me to the NASA Safety Advisory Group for Space Flight – was a no-nonsense visionary who withstood the lure of the technologically exotic by demanding that only *proven* hardware and concepts be employed in manned spaceflight.

Among the contributions that System Safety made to managing risk were the *widening of perspective* to an all-inclusive holism and *providing a systematic, proactive method* for risk control. However, System Safety – from its inception – suffered some unfortunate ills. First, it was misnamed. Using a common term “safety” in a brand-new way (that needed constant re-definition), it met stiff resistance from virtually everyone. Second, it focused equally on humans and hardware, when there was universal belief that safety was strictly *people-oriented* – not dealing with inanimate things. Third, it was shortly infected with the same numerical morbidity that had previously crippled Reliability – and began propagating a “dazzling display of deceptive decimals” in Fault Tree Analyses and Probabilistic Risk Assessments.

Therefore, executive reaction to System Safety soon matched that earlier accorded Reliability – namely that it was just another “technical cult” that exists only to satisfy an unspoken corporate/bureaucracy group ethic or *moralistic guilt*. While such cults have gained limited managerial acquiescence as useful for external (public) consumption, they have proven almost totally ineffective internally because management has never accepted them as *essential* disciplines. They are “nice but not necessary”. (Upon later exposure to Risk Management's full spectrum. I learned that the “nice but not necessary” epithet applies universally.)

5. Linking technological and financial

How did System Safety join the Risk Management spectrum? Jerome Lederer, renowned father of aviation safety and NASA's initial Director of Safety, first convinced me in 1967 that “risk management” was a more acceptable term to decision-makers than System Safety. Although I taught System Safety from 1967-85 at the University of Southern California, UCLA, and George Washington University, I was frequently interchanging Risk Management and System Safety in my courses – as concepts – by the early 1970's. In 1977,

I heard a taped lecture on Risk Management by H. Felix Kloman that convinced me to merge the two into a format that drew on the strengths of each.

Technological influence on Risk Management, based on the “hard” sciences, has proven significant by contributing aspects unique from anything at the financial end of the spectrum which is rooted in the “soft” sciences. Yet, while forcing a *maturation* and *expansion* of the subject, technology incorporation has not propelled Risk Management to its rightful niche in executive decision-making. In fact, technology’s revelation of risk’s complexity might have even (a) threatened some managers and (b) reinforced line management’s 40-year error of shirking its involvement in risk issues by delegating them to impotent staffs.

Though agreeing with Lederer and Kloman that Risk Management is the ideal descriptor for what executives need to do about loss potential, I continually face a major dilemma in using the term. It is inexorably bonded to and confused with *insurance* – that “last ditch” financial cop-out for failing to manage risk. It *presumes* losses rather than *preventing* them! A wide chasm divides what the term *says* from what it *does*. Upon reflection, it may be more misnamed than System Safety.

6. Remaining roadblocks

Why is Risk Management still widely unrecognized by executives? What continues to cause managers to view Risk Management as “nice but not necessary?” Why do decision-makers persist in making *benefit* decisions without making associated *risk* tradeoffs?

Impediments to Risk Management acceptance by executives – whether due to ignorance, misinformation, or prejudice – obviously abound. And they should be considered “*risks to managing risk*”. Therefore, they must be identified, evaluated, ranked, and eliminated/overcome just like any other risk. (Interestingly, the insurance industry would likely write a policy for *surviving* these impediments – instead of *eliminating/overcoming* them!)

How can an RMR (Risk-Management-Risk) best be identified? Perhaps by recognizing the characteristics of some current Risk Management indictments:

- a) Risk Management is a veiled come-on for insurance interests, a disguised sales gimmick supposedly offering clients some management assistance that actually provides insurers a plethora of insurance sales opportunities. (Have you ever wondered why there are more skyscrapers in major cities named after insurance companies than after any other business or industry?)
- b) In the public policy arena, Risk Management is a platform for political rhetoric designed to stampede legislators and taxpayers – through frightening environmental, health, security, and safety vagaries – into obsessive obeisance to “fear of risk”. (Have you ever been puzzled by esoteric profundities; e. g., radon in your shower, that are apparently intended to panic the average person but are obviously comprehended only by the alarmed expert?)
- c) Risk Management is a haven for all those who preach what “ought” to be done to make everything safe or secure without any concern for how much it will cost. (Have you ever mused whether safety experts *delight* in being able to morally pontificate free from any touch with economic reality?)

Of course, RMRs can also be identified by noting the behavior of executives who reject or ignore Risk Management:

- a) Risk Reaction must be superior to Risk Management – since it is the prevailing *modus vivendi* of business and industry. (Have you ever speculated about how EXXON found \$ 4.5 billion to pay for the EXXON Valdez disaster and yet never found the few dollars required to *avoid* or even *prepare* for an oil spill?)
- b) The historic “grab-benefit-first, fix-risk-later” syndrome is obviously mandatory – because it supports currently fashionable bottom-line mentality. (Have you ever pondered whether American automobile manufacturers are homesick for their cars because they continue to call them home?)

7. Roadblock evaluation

Are these formidable RMRs *insurmountable*? Should the Risk Management profession simply accept them as a “given” and proceed to live with them as one does with cancer? Can they be *ranked for significance* so that our always-limited resources are applied to overcoming the roadblock of greatest obstruction?

RMRs *can* be conquered – but only by those who are courageous enough to re-examine some very deeply-embedded tenets. It might seem that Risk Management simply needs a *bridge* from its time-honored principles to executive acceptance of those principles. But that would be a serious error. Both Risk Management and decision-makers have been travelling in the wrong direction for more than 40 years! Both parties must turn around 180°. This role reversal is described in *MANAGING RISK: Systematic Loss Prevention for Executives*.¹

Another sacred maxim requiring radical re-examination concerns the insurance industry – fountainhead of Risk Management. Neither intending to impugn nor be iconoclastic, I believe there likely is a “fox guarding the chicken house” – someone who claims to want to reduce a client’s losses but is actually profiting from those losses. Answers to these questions could either (a) verify that possibility or (b) destroy a major RMR:

- a) How does the insurance industry deny the obvious truth that – through its premium – it recovers the amount of a client’s loss, all associated administrative costs, *plus a profit*?
- b) Whose risks does the insurance industry *really* manage – their client’s or their own?
- c) What stimulus drives or forces the insurance industry to *reduce* client losses – rather than simply *accommodate* them or even *profit* from them through higher premiums?
- d) How – if at all – would the insurance industry differentiate (a) managing (i. e., identifying, evaluating, ranking, and controlling) a client’s risks and (b) assuring that a client has adequate financial recovery for a sustained loss?

8. Critical Incident Syndrome

Executive hindsightlessness is one RMR that shows promise of elimination – provided the Risk Management profession is successful in becoming systematic and all-encompassing. This RMR, known as Critical Incident Syndrome (CIS), is described as:

Intuitive and often overreactive response to a situation that has required management attention and correction for some time but continues to be neglected until triggered by

¹ Grose, Vernon L., *MANAGING RISK: Systematic Loss Prevention for Executives*, Prentice-Hall, Inc., Englewood Cliffs, N.J. (1987); 102-105.

an unexpected loss – personally or vicariously – of considerable magnitude, whereupon corrective resources previously unavailable are released in abundance.²

The onus for overcoming CIS rests, not with decision-making executives but with the Risk Management community which has failed to provide managers a rational framework for foreseeing the full range of loss potential. We have often acted as though risks were unforeseeable and unpreventable – with the only solution being to focus on *financial recovery from inevitable losses*.

This inexcusable mindset could be analogous to early medical practice when most deaths were attributed to “consumption” – for which there was no cure. That catchall was gradually deposed by defining specific infectious diseases which had been systematically and scientifically isolated one-by-one. Each was then attacked by inoculation, pharmaceuticals and surgery.

9. AIDS – A model for managing risk?

Recently, an exception to this successful medical pattern arose – and it might shed light on overcoming CIS. A solution for AIDS (acquired immuno-deficiency syndrome), the first “political” disease, is being pursued quite differently. Fundamentally, AIDS roots are behavioral rather than physiological. Those roots are widely-known, but public discussion of them is considered obscene. Instead of calling for root-eradication, mass media and public protests bombard society with the angry message that such causative behavior either cannot, must not or will not be changed. Nor, this tiny but strident minority insists, must society – for the first time in medical history – enforce any identification or isolation of the infected because of associated social stigma. Under the guise of “right to privacy”, the sick must remain free to infect (and intimidate) the well. Even diseased immigrants must not be denied entrance to the country and thereby access to infect others.

How is CIS related to the AIDS campaign? Its roots are also behavioral rather than technical, and just as simple to eradicate. Public discussion of CIS is uncouth, too. Underlying CIS, as with AIDS, is a very high “Know-Do” ratio as depicted in Figure 1. There is no shortage of *knowledge* – managers are simply short of *the will to do* what they already know would remedy the problem. Due to inordinate clamor for high yield on stockholder investment (similar to noisy AIDS advocates), executives lack the will to even *ponder*, ahead of time, what could go wrong – let alone invest in countermeasures against readily-identifiable losses.

If early death is the indicator for priority of cure, AIDS is a piker compared to death by automobile. Likewise, CIS post-event costs are orders of magnitude greater than preventive ones. So there is no *rational* argument to support either of these “intelligence-versus-action” gaps.

There is contrast in *advocacy* between AIDS and CIS, however. The few but militant voices for the AIDS-infected strive for public awareness while the numerous but passive advocates of CIS avoid public awareness. Notwithstanding this contrast, there is an

² Ibid., 387.

Figure 1:
The "KNOW-DO" Ratio

© Vernon Leslie Grose, 1974

unreality that must be flushed out and examined. Somehow, *truth and rationality are unsought* in both cases. Through political means, AIDS apologists have forced an inordinate amount of money and effort to be expended for an expensive secondary cure when the primary cure is virtually free. Through market economics, corporations have indulged the exorbitant CIS habit by passing on its totally unreasonable cost to taxpayers and consumers.

Why is the Risk Management profession obliged to equip decision-makers with a solution to CIS? Because, from its outset, it has had a vested interest in promulgating the inevitability of losses. The answer? Furnish executives with methodology which identifies – prior to occurrence – every conceivable type of risk (technical, legal, economic, social, environmental, and political) and then ranks their countermeasures for cost-effectiveness. That task demands awareness and commitment well beyond traditional *financial fascination* with risk. Be assured: CIS can be conquered, since it is always overcome when the human, political, and economic stakes are high enough. Examples include highway bridge construction, manned spaceflight, nuclear power generation, and commercial aircraft.

10. Key to every RMR: Behavioral change

To control Risk Management Risks, change is required. And all organizational change has – at its root – behavioral revision. Experts in achieving behavior transformation propose the five stages of essential elements listed in Figure 2.

First, you must catch their *attention*. Having done that – and while still holding their attention – you must get them to *comprehend* the message of change. But that's not enough. There is a difference between the comprehended message and their current behavior, so they must – as a willful commitment – *yield* their old way of behaving to the new. That new commitment must be *retained* as a part of their life-style until the appropriate time to take action that confirms the change.³

There must be a major re-structuring of Risk Management that openly integrates a full range of unacknowledged disciplines – political, cultural, social, behavioral, environmental, legal, historical – as elements that play a role in bringing about executive behavioral change. Those subconscious values that drive overt decisions must be reordered into a broader, more realistic paradigm.

*Figure 2:
Critical Elements of Behavioral Change*

11. Radical but proven solution

A systematic, all-encompassing methodology for Risk Management was developed – over a 20-year period – from a technological perspective. Its purpose? To eliminate or control RMRs by providing top management with a professional means for managing every type of risk. Known as SMART (Systems Methodology Applied to Risk Termination), it has been applied successfully in such diverse settings as telecommunications, hospitals, coal mining, condominium management, offshore oil drilling, and criminal justice. Even risks in designing the Washington, D.C. METRO were managed by SMART.

³ Ibid., 284-285.

Unique characteristics of SMART are summarized in Table 1. This technological product hopefully contributes missing infrastructure for integrating many commendable but disconnected elements in the Risk Management spectrum.

There is light at the end of the tunnel!

Table 1:
Unique contributions of SMART
(Systems Methodology Applied to Risk Termination)

Totally Integrated System – Allows technical, economic, political, legal, and social risks to be ranked into a single Hazard Totem Pole

Top Management Visibility – Graphic, quantified system for focused understanding of all risks by executives

Requires No Specialized Training – Non-mathematical, simple concept that can be universally understood

Organization-Wide Involvement – Literally everyone can contribute to the risk data base (supercedes most safety training!)

Non-Punitive Pursuit – Risk scenarios are “sanitized” by not naming people, organizations or other identities

Systematic, All-Encompassing Search – Every conceivable risk, regardless of perceived significance, is sought and managed

Client Ownership – Uniquely tailored to client needs and becomes an integral element of a client’s management system

Internal Risk Decisions – All client risks are identified, evaluated, ranked, and controlled exclusively by the client

Spill-Over Benefits – Functional models required for risk identification serve many other useful client purposes

Top-Down Control – Executives know their single most critical risk, their second, their third, and so on

Three-Dimensional Measure – The third dimension of risk (COST) joins SEVERITY and PROBABILITY for measure of risk significance

Wider Than History – Risks that have yet to happen can be readily integrated with existing incident and accident data