Let's Talk About Risk

Dennis Opacki, CISSP
July 5, 2007

Abstract

A person's perception of risk depends on his or her professional background, gender, age and environment. As a result, IT security practitioners often experience difficulty communicating security threats to executive management. The author examines several factors responsible for varying perceptions of risk, including recent findings in the fields of social psychology, neuroscience and behavioral economics. As a workaround, the author proposes the use of framing techniques to tailor security messages to a management audience.

Multiple Perspectives on Risk

Risk is everywhere. Analysts and statisticians measure and classify it. Hedge fund managers make fortunes trading it. Security professionals hyperventilate over it. Executives see it as a necessary tradeoff in the pursuit of greater rewards. All of these individuals have different views of risk and what they should do about it.

Financial Risk

Our success as IT security professionals may depend on understanding that the word *risk* has a different meaning, depending on a person's background and training. To people with backgrounds in finance, risk is not always bad. In fact, Merriam-Webster's dictionary defines the common business strategy of *speculation* as "assuming a business risk in hope of gain"[1]. Is it therefore any surprise that some CFOs and CEOs seem immune to IT security's constant admonitions of doom? How can they develop the business without assuming some risk?

In fact, in the financial world, the size of a risk is often proportional to potential gain. This explains why a person with a negative credit history pays a higher interest rate when borrowing money. Rather than simply canceling their risk by lending money only to creditworthy individuals, banks adjust borrowers' interest rates to compensate for their likelihood of default. Greater risk means a higher potential return.

Security Risk

So what does this mean for IT security? It means that, in our efforts to communicate with management, we have chosen terminology laden with some unfortunate baggage. As IT security professionals, our definition of risk better matches Merriam-Webster's, which

---

[1] "speculation." *Merriam-Webster Online Dictionary.* (2007). http://www.merriam-webster.com (23 May, 2007).

describes it as the "possibility of loss or injury"[2]. Among people with a security background, it often seems untenable to allow security issues to fester for the benefit of the business.

Bridging the Gap: Enter Framing

How can we compensate for different views of risk and management's seemingly insatiable appetite for assuming it? First, IT security personnel can adjust their language to talk less about risk and more about foreseeable threats to our brand, business and assets. We can then use a social psychological technique called *framing* to create compelling scenarios, which make threats seem more real (Kahneman, 2003).

Framing binds individuals' personal experiences and internal biases to the ideas presented through emotionally charged language. This is important because prospect theory, an area of behavioral economics, suggests that people base their choices largely on anticipated changes in emotional state (Kahneman, 2003). Thus, well composed frames can influence managers' decisions by eliciting vivid mental pictures of threat scenarios. For example, rather than stating that employees' personal information may be at risk, security professionals could frame the threat as follows:

An identity thief could steal a corporate laptop from a Human Resources employee in an airport or coffee shop. As our HR employees often store spreadsheets on their laptops, which contain the social security numbers and home addresses of employees, their spouses and dependent children, our staff and their families could unknowingly become victims of identity theft.

A Word of Caution: Ethics and Unintended Consequences

Framing IT security threats according to the principles of risk perception may seem like manipulation. However, it is similar to the communications tactics used in advertising, the news media and corporate communication. Whether framing is manipulative depends largely on intent. Security professionals should use framing judiciously and should consider their motives carefully. If the public disclosure of his or her techniques would embarrass the professional, or he or she would find it unacceptable for others to use similar tactics, the framing is likely unethical.

When used ethically, framing can be a powerful tool. However, it can also have unintended effects if mishandled. Unless IT security practitioners select frames carefully, they may undermine their own credibility or understate dangerous threats. Worldview, age, sex, emotions and environment play major roles in shaping peoples' views of risk. Understanding the basic psychology of the intended audience it is a precondition to the effective use of framing in risk communication.

---

[2] "risk." *Merriam-Webster Online Dictionary.* (2007). http://www.merriam-webster.com (23 May, 2007).

Risk Perception

How people feel about risk depends on several factors, including their backgrounds and worldviews, personal assessments of chance, and the affective value of likely outcomes. While the traditional pseudo-equation for risk incorporates likelihood and impact, noted risk communication scientists, Covello and Sandman, offer the following equation to better account for the emotional content of risk (Covello and Sandman, 2001):

$$Risk = Hazard + Outrage$$

Research shows the outrage surrounding a specific risk, as well as estimates of its likelihood and impact can vary widely by individual. Further, items such as gender, ethnicity and age contribute to the systematic overestimation or underestimation of risk. An outline of these factors follows.

Outrage Factors

In their 2001 paper on risk perception, Covello and Sandman suggest 20 factors, which influence peoples' risk estimates. The following are among the most relevant to IT security (Covello and Sandman, 2001):

- Voluntariness – People overestimate risks that they are not willful parties to.
- Familiarity – People overestimate risks that they are unfamiliar with.
- Trust – People overestimate risks related to parties they don't know or trust.
- Dread – People overestimate risks with disastrous or horrific outcomes.
- Media – People overestimate risks that receive disproportionate media attention.
- History – People overestimate risks that have occurred before.
- Identifiable victims – People overestimate risks that affect individual victims, rather than society at large.
- Effects on children – People overestimate risks affecting children.
- Personal stake – People overestimate risks that affect them personally.
- Reversibility – People overestimate risks that may have irreversible effects.

For example, it is clear to see why parents often overestimate the likelihood that a stranger will abduct their child on the child's way to school, despite statistical data showing that parental abductions are far more common. The scenario involves all 10 factors listed above. Further, most parents will agree that a better understanding of incident statistics does not ameliorate the outrage associated with such threats.

In general, IT security risks face a different challenge; many people underestimate the risks they face from computer criminals. This may be, in part, because computer users engage in risky behavior voluntarily. Further, an ability to change and customize their computing environment may also add to their feeling of familiarity with computer-related risks.

In addition, the Internet's current trust model is weak. Malicious attackers can use social engineering techniques to masquerade as familiar parties, or to subvert existing relationships. Evolutionary psychology tells us that, absent evidence to the contrary, it is

socially expeditious to give others the benefit of a doubt (The Economist, 2005). Unfortunately, when a computer user realizes that an attacker has subverted a trust relationship, the hacker has already achieved his or her goals.

Poor media coverage of IT security risks also contributes to underestimation of risk. However, identity theft seems poised to reverse this trend. A high dread factor, identifiable victims and the difficulty of reversing its effects make identity theft an instant media darling. Public dialog about unsafe computing practices, which enable identity theft, may increase the general outrage associated with computer crime.

Probability Estimates

Humans are notoriously bad at estimating the likelihood of rare events. In fact, most humans have difficulty conceptualizing probabilities other than 0 and 1 (Elster and Lowenstein, 1992). This binary view of probability may explain why humans spend so much time addressing yesterday's threats.

Until a new threat affects an organization, responsible parties often consider it purely theoretical and of negligible importance. Once it becomes a reality, the same parties assign it a likelihood of 1, and focus on how to prevent its recurrence. In effect, decision makers demand certainty, even when such data are unavailable (Covello and Sandman, 2001).

Research suggests that framing plays an important role in how people estimate probability. One study showed that people see risk as greater when they encounter likelihoods expressed as frequencies (10 chances in 100) versus percentages (Slovic, Monahan and MacGregor, 2000). The authors hypothesize that percentage estimates create a mental image of a single event, which the decision-maker can avoid altogether. Conversely, probabilities framed as frequencies bring multiple events to mind, some of which will surely affect the decision-maker.

Risk as Feelings

In their 2001 paper, *Risk as Feelings*, Loewenstein, Hsee, Weber and Welch draw a line between the effects of anticipatory and anticipated emotions on risk perception (Loewenstein et al., 2001). Like Kahneman, the authors believe that people base their decisions on the emotional content of expected outcomes. However, where prospect theory deals chiefly with anticipated emotions, those the decision-maker expects to experience immediately following a decision, Loewenstein et al. believe that anticipatory emotions, the feelings an individual experiences during the decision-making process, also play a significant role.

Circumstances such as the urgency of the decision, the decision-maker's mood, and "visceral factors" such as hunger and pain influence outcomes significantly (Loewenstein, 1996). In fact, when choices involve strong negative emotions, decision-makers may try to avoid decisions altogether (Luce et al., 1999).

Affective Value of Outcomes

Rottenstreich and Hsee extend prospect theory to account for the affective values of outcomes. In *Money, kisses and electric shocks: on the affective psychology of risk*, the authors describe how affect-rich outcomes, those associated with great hope or fear, can lead people to overweight low probabilities and underweight high probabilities (Rottenstreich and Hsee, 2001).

When the odds are against decision-makers realizing any result, they select choices with the highest potential impact. Even low-probability gambles seem palatable if their payoffs are large enough. Conversely, when presented with high-probability outcomes, decision-makers prefer affect-poor options, which they may characterize as "easy wins" or the "lesser of two evils".

Age Effects

Evidence is also gathering that peoples' sensitivity to risk changes as they age. One study used event-related functional magnetic resonance imaging to show that the caudate and insula, the regions of the brain believed to be responsible for the anxiety people experience when faced with a potential monetary loss, are less active in older adults (Larkin et al., 2007). However, older study participants experienced the same anticipatory emotions as younger ones when faced with potential gains; this may explain why some older adults engage in high-risk behavior or seem unreceptive to warnings of potential adverse outcomes.

While Male Effect

Other recent work suggests that white males assess risk differently than other demographic groups. Due in part to a more conservative worldview and a greater feeling of control over their environment, white males judge most risks as less severe than other groups (Finucane et al., 2000).

One recent study showed that 30% of white males judge most risks as extremely low (Finucane et al., 2000). Further, the study suggested the risk appetite of these "low-risk white males" does not depend on their education or experience. Instead, these individuals were skeptical of hazards, and more trusting of technology and institutions. This worldview may make this group less susceptible to outrage factors such as dread, trust and voluntariness (Covello and Sandman, 2001).

Conclusion

Framing can be a powerful tool for IT security professionals, who must bridge the semantic divide with executive management. However, practitioners must be careful not to exaggerate risk or communicate it in a manipulative fashion; this would be unethical. Instead, security professionals should know their audience and frame threats in terms that make them personal to decision-makers. With the proper tools and a basic understanding of human nature, IT security professionals can build much-needed consensus around risk within their organizations.

References

Covello, V., and Sandman, P. (2001). Risk Communication: Evolution and Revolution. In *Solutions to an Environment in Peril*, ed Anthony Wolbarst, pp.164-178. Baltimore, MD: John Hopkins University Press.

Elster, J., and Loewenstein, G. (1992). Utility from memory and anticipation. In G.F. Loewenstein and J. Elster (Eds.), Choice over time. pp. 213-234. New York: Russell Sage Foundation.

Finucane, M., Slovic, P., Mertz, C., Flynn, J., and Satterfield, T. (2000). Gender, race and perceived risk: the 'white male' effect. *Health, Risk and Society*. 2(2).

Kahneman, D. (2003). Maps of Bounded Rationality: Psychology for Behavioral Economics. *The American Economic Review*. 93(5).

Larkin, G., Gibbs, S., Khanna, K., Nielsen, L., Carstensen, L., and Knutson, B. (2007). Anticipation of monetary gain but not loss in healthy older adults. *Nature Neuroscience*. 10(6).

Loewenstein, G. (1996). Out of control: Visceral influences on behavior. *Organizational Behavior and Human Decision Processes*, pp. 272-292. 65.

Loewenstein, G., Hsee, C., Weber, E., and Welch, N. (2001). Risk as Feelings. *Psychological Bulletin*. 127(2).

Luce, M., Bettman, J., & Payne, J. (1999). Emotional trade-off difficulty and choice. *Journal of Marketing Research*, pp. 143-159. 36.

No Author Cited, (2005). Survey: The concrete savannah. *The Economist*, *377(8458)*.

Rottenstreich, Y., and Hsee, C. (2001). Money, Kisses and Electric Shocks: On the Affective Psychology of Risk. *Psychological Science*. 12(3).

Slovic, P., Monahan, J., and MacGregor, D. (2000). Violence risk assessment and risk communication: The effects of using actual cases, providing instruction and employing probability versus frequency formats. *Law and Human Behavior.* 24(3).