DOI:10.1145/2076450.2076462

Rose McDermott

Privacy and Security

Emotion and Security

Examining the role of human emotional response in making complex security-related decisions.

ILLUSTRATION BY GLUEKIT

Have you ever tried to convince someone to love you? Or has anyone ever tried to convince you to love them? A person can present the most logical and irrefutable arguments in the world about how well suited you are, how well you get along, how many critical values you share, and how complementary your interests and skills appear. The arguments may even be true. But the problem is you just don't feel it, so no amount of logic ever seems to overcome the lack of emotion. Conversely, if you feel the love, no amount of rational calculation can dissuade you, as the high divorce rate attests.

Security is like that as well. There is a reality to it. But there is also a feeling, right or wrong, that undergirds it as well. And those emotions are susceptible to manipulation, both strategic and accidental. Take, for instance, the U.S. Department of Homeland Security, and the myriad additional measures that have been put in place in airports since the attacks on 9/11 in order to make travelers feel more secure. Perhaps they actually also do make them more secure, but not as secure in actuality as efforts such as instituting consistent profiling and background checks on passenger lists that still remains largely anathema in a putatively democratic society.[7] Certainly committed terrorists could, with time and effort and ingenuity, overcome the procedural efforts put in effect by the TSA at airports by undertaking such deceptions as printing fake boarding passes.[8] Or they could find other, less well-secured targets against which to perpetrate their malfeasance. In the face of such reality, taking off increasing amounts of clothes prior to flying serves a primarily performative function, designed to induce complacency and a (false) sense of security. But as long as that feeling is real, it does not really matter if the reality does not exist. At least until these security systems fail to protect us from harm.

For good or ill, emotions do not always operate according to rational calculations. We are all aware of the impact of emotion on complex political, social, and economic processes through its influence on world markets in both bullish and bearish phases. Yet this reality also holds tremendous implications for both the public and policymakers when it comes to the issue of how threats affect how people think and feel about security as well—and how they act on it.

Take again, as an example, the influence of the color-coded alert system instituted by the Bush administration after the attacks of 9/11 on the mental and physical health of the U.S. population. As should be recalled, this system graded the security threat from green, associated with lower threat, to red, associated with high threat. When unspecified credible threats existed, the administration raised the level, and when intelligence indicated that threats appeared less imminent, the color level was lowered. Interestingly, a study of approximately 2,000 New York City Con Edison workers who serviced the areas in and around Ground Zero for several months after the attacks found that *lowering* as well as raising the alert level heightened serious symptoms of psychological distress, including increased arousal, depression, and anxiety.[5] Seemingly, just making the security threat more salient increases the negative outcomes associated with it.

Profiling Probability

The challenge presented by fear is that it does not tend to respond as probability theory might dictate. Probability theory suggests that a linear relationship should exist between the degree of threat and the likelihood and severity of response. But that is not what occurs. The implications of such findings pose a conundrum for policymakers. And in the case of cyberattacks and cyberexploitations, the problem is the emotions such as fear, or anger, can lead individuals to pay too much attention to the most obvious and visible threats, such as the risk of cyberattack, while paying insufficient attention, or completely ignoring, those areas where the risk is actually very high, and where greater vigilance really is warranted, such as the possibility of cyberexploitation.

In Prospect Theory models, individuals tend to weight probability not in the linear fashion advocated by standard normative models of probability theory, but rather by subjective functions that overvalue certain low-probability events, such as cybercrime, assigning them more psychological importance than they might otherwise merit, while simultaneously underweighting moderate and high-probability events such as cyberexploitation, rendering them less psychologically influential than they actually deserve. People also tend to place a great deal more importance on events that are deemed certain or impossible,[3] suggesting in part why so much emphasis is often placed in the public debate on identifying the perpetrators of particular events. Certainty justifies action and response in a way that uncertainty does not support.

Seemingly, just making the security threat more salient increases the negative outcomes associated with it.

Threats do produce some fairly predictable emotional responses in people depending on the emotion they elicit. The problem is it may not always be possible to predict which emotion will be generated in the face of any given threat by particular individuals. Evolution is a smart system, and some of the responses generated by fear, such as improved hearing and sight, especially in the dark, have aided survival.[2] This no doubt improves our ability to see predators, but may only cause anxiety disorders when the attackers are distant, unknown, or unknowable, as is typically the case in the realm of cybercrime. Furthermore, threats elicit different emotions in different people, with predictable divergence in downstream consequences. For example, women are more likely to experience fear, while men are more likely to experience anger. This matters because fear tends to generate withdrawal, and a tendency to avoid confrontations that might lead to an escalation of conflict, or a risk of blowback effects. Fear can make individuals pessimistic about their likelihood of prevailing in a conflict. On the other hand, anger tends to be quite activating, making individuals seeking vengeance quite optimistic about their prospects for victory against opponents.[4] Thus, policymakers will engender different levels of support for their proposed responses depending on whether they frame the threat as one that should induce fear or anger.

Communication Strategies

Nevertheless, there are certain strategies that decision makers can use that can prove more effective in communicating the appropriate level of threat and security risk to the public. Like Paul Revere's famous ride, credible threats should be communicated:

- by an expert and trustworthy source;
- it should be focused on a specific anticipated attack;
- it should motivate respondents to act; and

- it should provide specific concrete actions individuals should take to counter the threat.

In the realm of cybercrime, more effective and targeted communication strategies could help private citizens see and understand the difference between high-profile, low-probability events, such as non-state actors (terrorists) who might penetrate the Pentagon or major utilities, and low-profile high-probability events such as that presented by installation of malware on users' machines, compromising them. Such targeted communications strategies could also clarify the likelihood and risks of cyberexploitation, not only for holders of financial and identity information, but for any company that holds intellectual property, whether that is business plans, research and development work, patents, or other private information, including medical records.

Profound threats to security, of whatever form, can arouse deeply primitive responses in people for a variety of reasons, not the least of which is the way in which they make our own mortality salient to us. While prospects for cyberexploitation may not arouse thoughts of death in people who become victims, fear of hackers penetrating the launch codes of nuclear arsenals might easily do so. When death-related thoughts are made salient to people, they display heightened aggression toward those who threaten their world view.[1,6] And the group responsible for any given attack may not necessarily be the one targeted for the aggression that results from frustration and a sense of vulnerability.

Conclusion

In short, many responses, including preemptive responses to presumed threats or attacks, are emotionally based. These responses may not help protect the assets and values that are most important and that we hold most dear. In fact, overreacting to some threats, and not responding properly to others may result in our failing to protect ourselves as well as we might if we understood more about the nature of how uncertainty affects decision making and perceptions of actual risk.

Many responses, including preemptive responses to presumed threats or attacks, are emotionally based.

The academic community, as well as the interested and informed public, can help by more effectively communicating the nature of the objective risks posed form various aspects of cyber threat. And, more importantly, given the myriad real threats and challenges that face us individually and collectively, from climate change to pandemic disease to terrorism, more properly calibrating threat to response, and risk to fear in the area of cybersecurity, can allow all of us to put more time and attention into preventing and responding to the realistic threats that confront us, rather than chasing the unrealistic pursuit of existential security that eludes us all.

References

1. Cohen, F. et al. Fatal attraction: The effects of mortality salience on evaluations of charismatic, task-oriented and relationship-oriented leaders. *Psychological Science 15*, 12 (Dec. 2004), 846–851.
2. Cosmides, L. and Tooby, J. Evolutionary psychology and the emotions In M. Lewis and J.M. Haviland-Jones, Eds., *Handbook of Emotions, 2nd Edition.* Guilford, New York, 2000, 91–115.
3. Kahneman, D. and Tversky, A. Prospect theory: An analysis of decision under risk. *Econometica 47*, 2 (Feb. 1979), 263–292.
4. Lerner, J.S. and Keltner, D. Beyond valence: Toward a model of emotion-specific influences on judgment and choice. *Cognition and Emotion 14*, 4 (Apr. 2000), 473–493.
5. McDermott, R. and Zimbardo, P. The psychology of terrorist alarms. In B. Bonger, L. Beutler, J. Breckenridge, and P.G. Zimbardo, Eds., *The Psychology of Terrorism.* Oxford Press, New York, 2006.
6. McGregor, H. et al. Terror management and aggression: Evidence that mortality salience motivates aggression against worldview-threatening others. *Journal of Personality and Social Psychology 74*, 3 (Mar. 1998), 590–605.
7. Persico, N. and Todd, P.E. Passenger profiling, imperfect screening, and airport security. *The American Economic Review 95*, 2 (Feb. 2005), 127–131.
8. Soghoian, C. Insecure flight: Broken boarding passes and ineffective terrorist watch lists. *Policies and Research in Identity Management 261* (2008), 5–21.

Rose McDermott (Rose_McDermott@brown.edu) is a professor of political science at Brown University in Providence, RI.

Calendar of Events

February 16–17
International Symposium on Engineering Secure Software and Systems,
Eindhoven, Netherlands,
Contact: Etalle Sandro,
Email: s.etalle@tue.nl

February 20–22
The 6th International Conference on Ubiquitous Information Management and Communication,
Kuala Lumpur, Malaysia,
Sponsored: SIGAPP,
Contact: Sukhan Lee,
Email: lsh@exce.skku.ac.kr

February 22–24
Multimedia Systems Conference 2012,
Chapel Hill, NC,
Sponsored: SIGMM,
Contact: Mohamed Hafeeda,
Email: mhefeeda@cs.sfu.ca,
Phone: 778-782-7577

February 22–25
India Software Engineering Conference 2012,
Kanpur, India,
Contact: Professor Sanjeev K Aggarwal,
Email: ska@iitk.ac.in

February 28–29
Twelfth Workshop on Mobile Computing Systems and Applications,
San Diego, CA,
Contact: Gaetano Borriello,
Email: Gaetano@cs.washington.edu

February 29–March 3
The 43rd ACM Technical Symposium on Computer Science Education,
Raleigh, NC,
Sponsored: SIGCSE,
Contact: Laurie Smith King,
Email: lking@holycross.edu

March 3–7
Seventeenth International Conference on Architectural Support for Programming Languages and Operating Systems,
London, U.K.,
Sponsored: SIGOPS, SIGPLAN, SIGARCH,
Contact: Timothy L. Harris,
Email: tharris@microsoft.com