Transforming Apathy into Action: Applying Recent Research on Prosociality to the Culture of Security

by M. E. Kabay, PhD, CISSP-ISSMP
Professor of Computer Information Systems
School of Business & Management
Norwich University, Northfield VT

In 1993, I caused a stir in the world of information assurance by reviewing the applicability of well-established insights from social psychology to information assurance.< http://www.mekabay.com/infosecmgmt/Soc_Psych_INFOSEC.pdf > Apparently no one up to that time had bothered to make explicit reference to social psychology for insights into the management of information security. The work was revised for inclusion in the fourth and then in the fifth edition of the Computer Security Handbook.< http:// http://www.amazon.com/Computer-Security-Handbook-Volume-Set/dp/0471716529 >As my colleagues and I prepare for the publication of the sixth edition, due in October 2013, all of us are updating our chapters. Here's a paper that I am including in the social-psychology-and-infosec chapter in the next edition. As always, I am grateful to my dear father-in-law, Dr Percy Black, Emeritus Professor of Social Psychology, for his kindness in bringing this paper to my attention.

* * *

Emma F. Thomas< http://www.psychology.murdoch.edu.au/staff/thomas.html >, Craig McGarty< http://www.psychology.murdoch.edu.au/staff/mcgarty.html > and Kenneth I. Mavor< http://psychology.anu.edu.au/_people/people_details.asp?recId=126 > published an article in the November 2009 issue of *Personality and Social Psychology Review* 13(4):310-333 entitled "Transforming 'Apathy into Movement': The Role of Prosocial Emotions in Motivating Action for Social Change."< http://psr.sagepub.com/content/13/4/310.short > These Australian social scientists provide an extensive review of the literature on

- Evidence that membership in groups can support *prosocial*< http://learningtogive.org/papers/paper52.html > outcomes ("helping behavior, altruism, cooperation, and solidarity");
- Factors supporting prosociality in groups
- The roles of emotion (specifically guilt, sympathy and outrage) in fostering prosocial outcomes.

The authors' focus is on prompting action for social change in support of disadvantaged groups; however, there are implications for our work in encouraging employees to pay attention to security in their organizations.

One of the key findings of research on prosociality in the last four decades discussed by the authors is that "there are three core processes that underpin prosocial group behavior: category inclusion, category norms, and category interests."

- *Category inclusion* refers to how people see themselves as members of defined and inclusive groups. Thus if employees see themselves as belonging to "the company" or

"the organization" rather than solely as members of a smaller subgroup ("technical support" or "accounting") they may respond more favourably to attempts to stimulate prosocial behaviour such as identifying and reporting violations of security policy. Note that there is no conflict in belonging to both a sub-group and the more inclusive group; the issue is whether a person sees any common identity with the larger group.

- *Category norm*s refers to expected or normative behaviours for a group. These norms are explicit articulations of values; for example, "We really ought to report a stranger who is walking about in a restricted area" could be a category norm for the security team; the challenge is to extend this norm to the wider class of all employees.
- *Category interests* are "the strategic concerns that accompany helping behavior." For example, convincing employees that their own personal reputations and the reputation of the entire company are threatened by security breaches would be a development of a category interest.

Emotion plays an important role in moving people towards concerted action (social *action*). The authors point out two ways that emotion can lead to social action:

- Identification as a member of a distinct group can lead to shared (group) emotion – shared feelings (positive or negative) about issues – which in turn can lead to social action.
- Individual emotions can lead people into identifying themselves with social groups and again, lead to social action.

In our security context, perhaps we can build on these two sequences. For example, fostering group identity using such tools as, say, t-shirts with a company logo or motto (with or without additional subgroup individuation such as the addition of , say, "tech support" or "security team") or by hosting social events to which all members of the organization are invited (as opposed to having only members of a specific department attend) could solidify group identity. The other approach would involve articulation of group values that could attract employees into self-identification with the social identity. In my experience, for example, Hewlett-Packard (HP) in the 1980s was successful in fostering a set of shared values, starting with "People are our number 1 resource." I have often told students about how, in 1982, a recession decreased sales significantly for HP worldwide; upper management circulated an announcement to all HP offices worldwide starting that the company had to cut salary expenses by 10% -- but instead of firing 10% of the 87,000 employees at that time, they reduced *everyone's* salary by 10% and offered us all every second Friday off as an unpaid holiday. In the office where I worked (#2012 in Kirkland, Quebec), not one employee quit – and no one took the free Fridays, either. Instead, we worked like blazes to serve our customers (I was a systems engineer in the HP3000 group at that time) and to advance our internal training. By 1983, when the economy turned back up, we were 'way ahead of our main competitors, who had to scramble to hire and train new employees. In those years, HP consistently won J. D. Powers awards for customer service.

In terms of category inclusion, the authors write, "groups' emotions have the potential to shape and restructure (inter)group boundaries. For example, experiencing feelings of fear in relation to another person is unlikely to lead to a categorization of that person as an in-group member…." In contrast, several lines of research support the view that when people share the same emotions, they may strengthen their group identification. In the security context, perhaps we can articulate the legitimate threat from criminal hackers, industrial spies, and attackers sponsored by nation-states to strengthen dislike of these out-groups among our employees. I am not proposing exaggeration and propaganda here: providing accurate descriptions of the depredations of these

attackers should suffice to support increased group identification and therefore increased willingness to take action in defence of the group.

The authors review work by several scientists suggesting that "anger plays a powerful role in politicizing a social identity, transforming the identity such that it is more ready for social action." Perhaps more explicit reference to the cultures and threats of the attackers could have positive outcomes in solidifying group identify among our employees and supporting active responses in support of information security. For example, expressing anger at organized cybercrime syndicates< http://money.cnn.com/2011/07/27/technology/organized_cybercrime/index.htm > such as the Russian Business Network (RBN)< http://www.spamhaus.org/rokso/evidence/ROK7740/russian-business-network/media-a-walk-on-the-dark-side > that was active during the mid-2000s< http://www.spamhaus.org/rokso/evidence/ROK7740/russian-business-network/media-a-walk-on-the-dark-side >. Providing educational material detailing current attackers' behaviour and emphasizing that we are justified in expressing anger at their illegal actions may be a positive contribution to encouraging more prosociality to support increased vigilance and readier reporting of clues to suspicious activity on our systems.

Research into category interests supports the view that "emotions will shape the sorts of strategies that group members prefer… in particular depending on where the emotion implies that blame lies (one of the key appraisal categories…)." So perhaps in our security briefings, a bit more visible outrage about the culture and bad behaviour of our attackers may actually contribute to reinforcing the willingness of our colleagues to engage in better defences. Instead of maintaining a detached objectivity about cyberscum (!), we may be better off letting our indignation show through during training and awareness sessions.

Other sections of the authors' article cover details of prosocial emotions (guilt, sympathy, and moral outrage) and also of self-focused anger as factors affecting prosociality. Some of the key findings of particular relevance to information security are as follows:

- *Guilt* refers to feelings of responsibility for behaviour or situations which are viewed as negative, harmful, wrong or immoral. Interestingly, "it is possible to induce guilt in people even though their personal self was not responsible for the harm inflicted on another." Perhaps a security trainer who expresses regret over the loss of reputation experienced by a victim of q stolen password lost by responding to a phishing e-mail can parlay this sense of responsibility into a group acceptance of an evolving moral norm: it is "wrong" (not just silly or careless) to be unaware of common techniques for identity theft. However, guilt is not viewed as a powerful motivator of prosocial behaviour; indeed, "there are at least three ways that individuals can avoid the experience of group-based guilt: They can minimize the harm that was done to the other group, question the appropriateness of guilt, and engage in argument about the cost of apology…."
- *Sympathy* is "heightened awareness of another's plight as something to be alleviated…." Sympathy seems to be a strong motivator for both "interpersonal…and intergroup prosocial behavior…." Perhaps focusing on the personal consequences of specific or typical victims of breaches of security (e.g., suspicion cast on an innocent victim of password theft) could support behaviours to reduce the occurrence of such security breaches. However, it seems to me that it would be unwise to express sympathy for cybercriminals, regardless of their motivations.< http://www.cyberwarzone.com/cyberwarfare/pinoy-hackers-scale-attacks-china-websites >

- *Empathy*, distinct from sympathy, is a move towards increased identification with the other; thus in our context of information security, awareness and training sessions my benefit from emphasizing the commonality of all victims of cybercrime. Instead of feeling bad for other people, an empathic response would move employees to see themselves as potential victims. Perhaps we could explicitly engage in role-playing to encourage our colleagues to articulate how they would feel as the victims of various cybercrimes.

The paper has much more of interest for those of us working on security awareness and training, and I recommend it highly.

Those with access to academic libraries will find it easy to locate paper or electronic versions of the article at no cost to them. However, the publisher does make the article available as a downloadable PDF – for the usual exorbitant fee (in this case, U$25), illustrating as always the notable commitment of commercial publishers to the advance of human knowledge – by receiving articles without payment to the authors, receiving scholarly reviews of the manuscripts without payment to the reviewers, and asserting exclusive ownership of the published articles.

* * *

M. E. Kabay,< mailto:mekabay@gmail.com > PhD, CISSP-ISSMP, specializes in security and operations management consulting services and teaching. He Professor of Computer Information Systems in the School of Business and Management at Norwich University. Visit his Website for white papers and course materials.< http://www.mekabay.com/ >

* * *