DOI:10.1145/1978542.1978544

A Policy that Deters Violation of Security Policy

IN THEIR ARTICLE “Does Deterrence Work in Reducing Information Security Policy Abuse by Employees?,” Qing Hu et al. (June 2011) analyzed deterrence of employee violation of information-security policy based on various criminological theories. Along the same lines, some years ago, when I interviewed more than 200 information security abusers,³ I found one of Donald R. Cressey’s criminological theories especially useful.¹ Cressey deduced from interviews of several hundred convicted embezzlers that mostly they were motivated by wanting to solve intense, non-shareable problems, exceeding the limits of their moral beliefs of right and wrong and self-control.

The survey Hu et al. described in their article, asking what a random sample of employees would do given several scenarios, is not particularly meaningful in the absence of the intense stress and highly variable conditions and circumstances I found to be present in cases of actual violation. In addition, perpetrators often find it easier to act against emotionless and faceless computers and prosperous organizations than directly against their fellow humans. Computers don’t cry or hit back, and, as perpetrators rationalize, organizations can easily help solve their problems and write off any loss.

Unfortunately, Hu et al.’s model did not include avoidance, separating or eliminating potential threats and assets, along with deterrence, leading only to the obvious advice of proactively hiring people with strong self-control and high moral standards. Organizations don’t knowingly hire people with such deficiencies; rather, employees become deficient under conditions and circumstances that emerge only during their employment. I concluded that providing employees in positions of trust free, easily accessible, confidential, problem-solving services is an important information-security safeguard,² sub-

sequently recommending it to many of my clients.

Donn B. Parker, Los Altos, CA

References

1. Cressey, D.R. *Other People’s Money*. Wadsworth Publishing Company, Inc., Belmont, CA, 1953.
2. Parker, D.B. *Fighting Computer Crime, A New Framework for Protecting Information*. Wiley, New York, 1998.
3. Parker, D.B. The dark side of computing: Computer crime. *IEEE Annals of the History of Computing* 29, 1 (Jan.–Mar. 2007), 3–15.

Authors’ Response:

We appreciate Parker’s critique of our approach to studying corporate computer abuses. Including known offenders in such a study would certainly be desirable. However, including the general population in any study of criminal behavior is a proven approach in criminology, as was our approach of using randomly selected office workers who may or may not have committed some kind of abuse. Both approaches are needed to better understand the complex social, economic, and psychological causes of employee abuse against their employers’ systems.

Qing Hu, Ames, IA,
Zhengchuan Xu, Shanghai,
Tamara Dinev, Boca Raton, FL,
Hong Ling, Shanghai

Agility Sometimes Another Extreme

I commend Phillip G. Armour’s Viewpoint “Practical Application of Theoretical Estimation” (June 2011), as I’m always on the lookout for ideas concerning software estimation, even as I ponder my own eternal mantra: “Estimates are always wrong.”

I agree with Armour but think he missed an opportunity in his section labeled “Practicing the Theory” to emphasize how agile methods avoid the extremes of compression and relaxation. Relaxation is avoided by breaking traditionally slow-to-deliver projects into small agile pieces, each easily delivered within the related market window. Working with these pieces also serves to avoid compression, since the same number of people can deliver the smaller agile pieces more quickly.

Armour also did say this is all theoretical and that even under the guise of agility companies regularly try to ramp up too many agile pieces too quickly.

Geoffrey A. Lowney, Issaquah WA

Communications welcomes your opinion. To submit a Letter to the Editor, please limit yourself to 500 words or less, and send to letters@cacm.acm.org.

© 2011 ACM 0001-0782/11/08 \$10.00

Coming Next Month in COMMUNICATIONS

**Protecting Users
of the Cyber Commons**

**The Future of Wireless
Data Communications**

**Realizing the Value
of Social Media**

Code Bubbles

**Qualitative Analysis
of Real-time Systems Using
Priced-Timed Automata**

**Satisfiability
Modulo Theories**

**And the latest news about data breaches,
mobile app ecosystems, and solving systems of linear equations.**