Methods for evaluating and effectively managing the security behavior of employees.

BY QING HU, ZHENGCHUAN XU, TAMARA DINEV, AND HONG LING

Does Deterrence Work

in Reducing Information Security Policy Abuse by Employees?

HACKING INTO CORPORATE IT systems and individuals' computers is no longer a sport for bragging rights, but a major organized economic activity aiming for significant profits controlled largely by underground networks of criminals and organized crime on a global scale.² The financial impact of the computer crimes and related activities is estimated at over one trillion dollars each year worldwide.¹⁷ Unfortunately, despite significant advances in hardware and software technologies against computer and network offenses, in the digital security ecosystem around any organization, human agents are still the weakest link in the defense against outside attacks and the most dangerous to the organizations from within. Indeed, the effectiveness of other elements in the

security system, such as security technology, organizational policies and procedures, as well as government regulations, are largely dependent on the effort of the human agents, especially those who work within the organizations.

While the media headlines tend to focus on the spectacular events perpetrated by external hackers, employees inside an organization often pose silent but more dangerous threats than those outside the organization,³⁰ due to their intimate knowledge about the organizational systems and the permissions they receive either properly or improperly for their work activities. In a recent survey of IT managers of global companies, 60% of the respondents said employee misconduct involving information systems (IS) is a top concern about information security.¹¹ The 2008 CSI Computer Crime and Security Survey shows that 44% of respondents reported insider abuse of computer systems, making it the second most frequent form of security breach, only slightly behind virus incidents (49%), but well above the 29% of respondents who reported unauthorized access from external sources.²²

In this study, we focus on information security policy violations by employees in organizational settings. Employee information security policy violations vary widely in motives, forms, targets, and consequences. We define information security policy violation as any act by an employee using computers that is against the established rules and policies of an organization for personal gains. By this definition, information security policy violations include but are not limited to unauthorized access to data and systems, unauthorized copying or transferring of confidential data, or selling confidential data to a third party for personal gains, and so forth. With this focus, two questions have been central to research and practice in information security in the last two decades: Why do employees go rogue and commit policy violations, and what could

employers do to minimize the threat and the damage? Recent research^{8,10,25} based on human behavioral theories has made two primary recommendations: implement comprehensive information security policies and procedures and conduct thorough awareness training for employees, and establish clear and swift sanctions against security misconduct to deter and reduce future violations by employees. Surveys^{11,22} indicate these recommendations have been widely adopted and implemented by companies, yet the threat of policy violations remains a top concern of information security management. In this article, we highlight a study conducted by the authors in an effort to understand the mystery and provide better insights into security management practices. We set out to extend the current re-

search on the behavioral aspects of information security and attempt to accomplish three objectives: to integrate multiple theories to develop a comprehensive model about security misconduct behavior in corporate settings; to test the causal relationships among rational choice, deterrence, individual propensity, and security misconduct behavior of individuals; and to provide prescriptive guidance to information security management based on the results of this research.

Criminological Theories of Human Behavior

The significant role of human agents in organizational information security has long been recognized by scholars, along with the effort in developing and deploying more advanced protective technologies and establishing and en-

forcing effective security policies and procedures. Early studies of information security by IS scholars were largely based on surveys of managers and employees in organizations using ad hoc theoretical or empirical frameworks. Only recently have IS scholars started to use more established theories in their analyses of the information security issues (for example, D'Arcy,⁸ Dinev,¹⁰ Siponen²⁵). Given the similarity between information security policy violations in organizational settings and criminal behavior in social settings, the theories and theoretical perspectives developed in criminology literature have been widely adopted as the foundations for information security research, including but not limited to deterrence theory, rational choice theory, and social control theory. Table 1 summarizes the main

thesis of the most relevant theories for this study.

Although rational frameworks have been popular in criminology literature, they are often used in conjunction with other theoretical frame-

works. Since human beings are only capable of bounded rationality,²⁴ it is reasonable to assume the rational decision-making process will be subject to a variety of individual and situational factors. Paternoster and Simp-

son¹⁹ emphasized that the rational choice theory of crime is essentially a subjective expected utility theory that has two assumptions: decisions by an individual to offend are based on the evaluation of cost and benefit of offending; and the critical elements in this calculus are the perceived or subjective expectations of cost and benefit by the individual. Therefore, the cognitive characteristics of the individual and the specific characteristics of the situation will affect how the benefit and cost are perceived.⁷ Tibbetts and Gibson²⁸ found that studies with both the rational choice measures and the estimates of individual propensities show that variables from these two perspectives significantly influence the deviant behavior, even when factors from other theoretical perspectives are controlled.

The literature review led us to propose a research model with the rational choice at its core and other theoretical frameworks at its periphery to form a theoretical model of information security policy violation behavior. The treatment of individual propensity, moral beliefs, and perceived deterrence as antecedents to the rational choice calculus may be debatable, but is primarily based on the findings of criminological studies (for example, Nagin,¹⁸ Piquero²¹) that use rational choice theory as the foundation for human behavior, as well as our preliminary testing that showed insignificant moderating effects by these three constructs on the rational choice theory model. We submit that when an individual is presented with an opportunity to commit policy violations, his or her behavior depends on the rational calculus of the costs and the benefits. However, the mechanisms of the cost-benefit evaluation are affected by at least three independent forces: two internal and one external to the individual. The two internal forces are the individual propensity (defined as the degree of low self-control), and the individual's moral beliefs (defined as the individual's judgment about right and wrong). The external force is the perceived deterrence related to the misconduct, defined as the perceived certainty, severity, and celerity of sanctions against the behavior. We argue that low self-control, moral beliefs,

Table 1. Highlights of relevant criminological theories.

Theory	Type	Description	Primary Sources
Rational Choice	Behavioral Theory	<ul style="list-style-type: none"> Individuals are sensitive to the consequences of their actions and make reasoned judgments based on the cost-benefit analysis of the intended acts. The decision to engage in criminal behavior is a function of the perceived costs and benefits of the criminal act. 	Becker ⁵ Cornish ⁷ Paternoster ¹⁹
Self-Control	Behavioral Theory	<ul style="list-style-type: none"> All human beings have the potential of committing crimes, but not everyone does because of differences in the ability of self-control. Self-control is established early and remains relatively stable throughout an individual's lifetime. Individuals with low self-control have a tendency to respond to tangible stimuli in the immediate environment, and are more likely to be seduced by the thrill and excitement of criminal acts. 	Gettfredson ¹²
Deterrence	Behavioral Theory	<ul style="list-style-type: none"> Human beings are fundamentally rational in their behavior and choose crime only when it pays. Individuals are less likely to commit criminal acts if the perceived certainty, severity, and celerity of sanction against the acts are greater. 	Gibbs ¹³ Tittle ²⁷
Shame	Behavioral Modifier	<ul style="list-style-type: none"> Shame is the experience of temporary loss of self-esteem in an internal evaluation of the self by an individual. Shame has a deterrence effect on various criminal acts through three mechanisms: self-imposed shame (or shame), socially imposed embarrassment, and state-imposed legal sanctions. 	Lewis ¹⁶ Piquero ²¹
Moral Beliefs	Behavioral Modifier	<ul style="list-style-type: none"> Moral beliefs are individual judgment of right and wrong about specific behavior. Moral beliefs against committing criminal acts increase the degree of perceived sanctions and the shame associated with the acts. Moral beliefs also have a negative effect on the perceived pleasure from the deviant behavior. 	Bachman ⁴ Piquero ²¹

Figure 1. Conceptual model.

and deterrence are antecedents of the rational choice calculus rather than moderators as seen in some studies (for example, D'Arcy,⁸ Paternoster¹⁹). This is because we believe these factors are more likely to change how the benefits and costs are assessed rather than how the benefits and costs are weighed in the decision calculus by an individual. For instance, an individual with strong moral beliefs is likely to underestimate the benefits while over-estimating the risks of the misconduct. Similarly, an individual with low self-control seeking immediate thrill and excitement is likely to overestimate the benefits while underestimating the costs of committing the act. This thesis leads to the formulation of the integrated model of information security policy violation by internal employees, as shown in Figure 1.

Testing the Theory

Due to the secrecy involved in criminal or deviant behavior, it is natural that individuals will be unwilling to report their actual behavior and actions related to policy violations or crimes. In criminology and IS security research, faced with this difficulty, scholars have often resorted to the use of scenarios of criminal or abusive activities to elicit input from survey subjects. In this study, we adopted the scenario-based survey methodology to collect data from employees in organizations who may or may not have committed policy violations toward corporate computer systems. Using scenarios to elicit individual responses has been a common technique in criminology research (for example, Bachman,⁴ Paternoster,¹⁹ Piquero²¹), and it has been increasingly used by IS scholars in information security research (for example, D'Arcy,⁸ Siponen²⁵).

The constructs shown in the conceptual model were operationalized into latent variables that can be measured using a survey instrument, as shown in Table 2. The survey instrument was developed based on the proposed conceptual model after the constructs were operationalized into measurable items with a 7-point Likert scale. All of the items were adapted from the extant literature in order to maximize the validity and reliability of

the measurement model. Three carefully designed information security policy violation scenarios were presented to each respondent at the beginning of the survey to elicit his or her intention to do the same as the actor did in each of the scenarios. The scenarios included unauthorized access to payroll data, unauthorized access to and transfer of product designs, and stealing and selling confidential price and cost data to competitors. A validation question that asks the respondents about how likely the scenarios could occur in their companies was included after each scenario.

The survey was pilot tested using EMBA students enrolled in a major Chinese university. Oral comments were collected and diagnostic statistics were conducted. Minor revisions were made based on the results of the pilot test. The final survey was distributed to employees in five large organizations in China. These organizations were selected largely due to their willingness to cooperate with this

research after the authors contacted a number of organizations. Primarily because of the supportive arrangement of the managers of these five organizations, the response rate of the survey was nearly 100% from about 50 randomly selected employees in each organization. The surveys were distributed and collected by the research team directly in a meeting room setting at each location. The employees were assured the management would not have access to the individual surveys. In the end, 227 surveys were received, 207 were deemed as complete and usable, 20 were discarded due to incomplete answers. More than 79% of the respondents were younger than 35 years old, and more than 71% had a college or higher level education, reflecting a young and well-educated work force in these organizations. Over 75% of the respondents classified themselves as "employee" as opposed to having supervisory responsibilities. Of the respondents, 58% were male, and 42% were female, reflecting a typi-

Table 2. Operationalization of theoretical constructs.

Theoretical Construct	Latent Variables	Description
Individual Propensity	Low Self-Control (LSC)	Measured as a combination of the impulsivity, risking seeking, and self-centered characteristics of an individual.
Individual Moral Beliefs	Moral Beliefs (MRB)	Measured in terms of how morally wrong and morally unacceptable the intended act is to the respondent.
Perceived Deterrence	Perceived Certainty of Sanctions (CRT)	The perceived probability of being punished for the intended act.
	Perceived Severity of Sanctions (SVR)	The perceived degree of punishment for the intended act.
	Perceived Celerity of Sanctions (CEL)	The perceived swiftness of being punished for the intended act.
Rational Choice Calculus	Perceived Extrinsic Benefits (PEB)	The perceived material benefits of committing the intended act.
	Perceived Intrinsic Benefits (PIB)	The perceived mental pleasure of committing the intended act.
	Perceived Formal Risk (PFR)	Measured as the product of how likely and how much a problem are the formal sanctions—loss of job and face legal action—to the respondent.
	Perceived Informal Risk (PIR)	Measured as the product of how likely and how much a problem are the informal sanctions—loss of respect from family, relatives, friends, and colleagues—to the respondent.
Behavioral Intention	Perceived Risk of Shame (SHM)	Measured as the product of how likely and how much a problem they are—losing self-esteem and feeling of guilt about the intended act—to the respondent.
	Intention to Commit Violation (INT)	Measured in terms of how likely and how willing the respondent would do what the fictitious characters did in the specific scenarios.

cal gender composition in these organizations.

To analyze the measurement quality as well as the path model for hypothesis testing, we used SmartPLS²³ as the primary statistical tool. Following the widely adopted two-step approach to structural equation modeling,^{3,15} we first assessed the quality of the measurement model to ensure the validity and reliability of the construct measurements. This was followed by structural modeling to test the research

hypotheses and the overall quality of the proposed model. The primary indicators for quality of the structural model are the R^2 values of the endogenous variables,¹⁵ which measure how much of the variances in the endogenous constructs are explained by the exogenous constructs specified in the model. The R^2 value for the dependent variable, INT, is 0.337, indicating that the variables in the model explained about 34% of the variance in the dependent variable, which, by the stan-

dard of structural equation modeling, is moderately high when compared to published studies (for example, D'Arcy⁸). Figure 2 presents the results of the structural analysis.

Does Deterrence Really Work?

The interesting results from this structural model are about the individual calculus that leads to the intention to commit policy violations toward computer systems in organizational settings. The hypotheses related to the impact of perceived benefits (PEB $\rightarrow$ INT, $\beta=0.149$, $p < 0.05$ and PIB $\rightarrow$ INT, $\beta=0.328$, $p < 0.01$) are supported, while the hypotheses related to the perceived risks (PIR $\rightarrow$ INT, $\beta=-0.201$, $p > 0.1$ and PFR $\rightarrow$ INT, $\beta=-0.005$, $p > 0.1$) are not supported. This result suggests that when an individual is contemplating whether to commit policy violations, the perceived benefits dominate the perceived risks in the rational decision-making process. The significant path from PIB to INT suggests the individual's intrinsic satisfactions that would be gained from the misconduct, such as thrill and happiness, are even more influential than the extrinsic material gains, such as the possession of money and goods, on the behavioral choice of the individual.

Perhaps equally interesting is the insignificance of the hypotheses related to deterrence, which is modeled as a second order formative construct of certainty, severity, and celerity of sanctions against the policy violations. Our results show the deterrence has no significant impact on individual intention to commit policy violations. While the deterrence does impact the perceived informal risk ($\beta=0.209$, $p < 0.05$) and perceived formal risk ($\beta=0.281$, $p < 0.01$), such impacts apparently do not have a significant influence on the individual's intention to commit the violations against the established information security policies.

These results seem to contradict, at least partially, the prevalent view about deterrence in the information security literature and practice. To be sure, we also tested a straightforward deterrence model in which only the three deterrence constructs (certainty, severity, and celerity) were directly linked to the INT construct. The result is shown in Figure 3. All path coeffi-

Figure 2. Results of structural analysis.

(***, **, and * indicate statistically significant at $p < 0.01$, 0.05 , and 0.1 levels)
 (LSC-low self control, MRB-moral beliefs, DET-deterrence, PEB-perceived extrinsic benefits, PIB-perceived intrinsic benefits, SHM-perceived risk of shame, PIR-perceived informal risks, PFR-perceived formal risks, INT-intention to commit computer misconduct)

Figure 3. Testing of deterrence effect.

(NS indicates not statistically significant)
 (CRT – certainty of sanction, SVR – severity of sanction, CEL – celerity of sanction, INT – intention to commit policy violations)

cients were found to be insignificant and the total variance explained is less than 6%. This result clearly suggests deterrence alone will not be effective, at least in the sample population of this study, in terms of reducing employee information security policy violations.

These results are consistent with the findings of Tunnell²⁹ in a criminology study that criminal offenders primarily think about positive consequences and little about negative consequences—approximately 60% of the criminals interviewed said they simply did not think about the possible legal consequences of their criminal actions before committing the crimes. Interestingly, studies on user behavior at online social networking sites^{1,9} found similar results that the benefits of social networking outweigh the risks of privacy concerns and users seem to ascribe the risks more to others than to themselves. A recent study by Siponen and Vance²⁵ showed deterrence mechanisms are not effective in the presence of neutralization mechanism in reducing security policy violations. This raises some critical questions: Why do benefits dominate risks in the rational calculus of individual behavior? How can the risks be accentuated? And why are the risks often ignored? We don't have answers to these questions and they will be the focus of our future research on information security.

While our model explains why deterrence may not be effective, it also shows what does work in reducing the policy violation intentions of employees: self-control and moral beliefs. Although moral beliefs have a strong impact on the perceived intrinsic benefits ($\beta=-0.163$, $p<0.05$), shame ($\beta=0.462$, $p<0.01$), perceived informal risk ($\beta=0.413$, $p<0.01$), and perceived formal risk ($\beta=0.352$, $p<0.01$), their impact on the policy violation intention is dampened somewhat because only the perceived benefits have significant impacts on the policy violation intentions. Nonetheless, the strong negative causal chain from moral beliefs to perceived informal risk to violation intention makes moral beliefs an important factor in the rational calculus of employees for committing policy violations.

Individuals with low self-control are more likely to be tempted by the appeal of the violations in terms of perceived benefits, and thus more likely to commit the acts.

The role of low self-control in shaping employee policy violation intentions is explained by our research model and confirmed by the data. Individuals with low self-control are more likely to be tempted by the appeal of the violations in terms of perceived benefits, and thus more likely to commit the acts. This is because low self-control leads to higher levels of perceived extrinsic benefits ($\beta=0.150$, $p<0.1$) and perceived intrinsic benefits ($\beta=0.393$, $p<0.01$), which in turn strongly influence the intention to commit the policy violations ($\beta=0.149$, $p<0.05$ and $\beta=0.328$, $p<0.01$).

What Can Employers Do?

While the results suggest deterrence may not work as effectively as many scholars and practitioners have believed, our findings suggest at least two directions for effective management of employee information security behavior: lowering the perceived benefits of committing the violations, and screening applicants with a high level of self-control and strong moral beliefs for sensitive positions. To lower the perceived benefits of violations against corporate information security policy, companies can take a number of proactive actions to reduce the perceived value of the data assets in corporate information systems. Data assets with high perceived value, such as customer records, credit card numbers, and confidential product designs, attract attention from internal and external entities and thus increase the chances of being misappropriated. Making data assets less attractive to potential offenders is difficult but not impossible. For example, a company could choose not to store customer credit card numbers on its servers (in most cases such storage is not necessary for completing financial transactions), protect confidential data with strong encryption systems, and distribute sensitive data to multiple secure servers (physical or virtual) with different layers of protection and access mechanisms, such as using different operating systems and security software and hardware from different vendors.

For positions where access to highly valued data assets must be authorized, companies should consider screening

applicants using psychometric instruments to ensure that only those who are strong on self-control and have compatible moral beliefs are assigned to these positions in addition to their technical qualifications and job responsibilities. Employees with low self-control could well be productive, innovative, and valuable in appropriate positions, but should not be assigned as custodians of sensitive data assets. On the other hand, the moral beliefs of employees can be strengthened by adopting high standards of organizational ethics and corporate citizenship. This is because organizations with strong ethics attract and retain employees with high moral standards.⁶ By recruiting and retaining employees with high moral standards, companies may reduce the chances for information security policy violations committed by employees.

Conclusion

In this article, we described a comprehensive model of information security policy violation by employees in organizational settings based on multiple criminological theories. We presented the results of empirical tests of this model and the implications of the findings for information security management theory and practice. While we cannot claim we have unlocked the mystery of why deterrence is not effective in reducing policy violations, we shed some light on this complex and significant issue. We found that while the rational choice framework of deviant behavior is largely supported, the perceived benefits of violations often dominate the perceived risks in individual decision calculus. As a result, the deterrence antecedents are less effective than the self-control and moral belief antecedents in shaping individual behavior.

With this understanding of employee information security behavior, our results reveal what might help companies effectively reduce the policy violations by employees: lowering the perceived value of the data assets in corporate information systems, and screening for individuals with high self-control and high moral standards. We find that individuals with low self-control, those who are more concerned about themselves

than others, more interested in what happens now than in the future, and more risk taking than risk averse, are more likely to overestimate the benefits of the misconduct. On the other hand, employees who have strong moral beliefs about right and wrong are less inclined to commit the violations even when the opportunities are presented. We believe this type of prescription for information security management has not been presented before and could have a significant impact on information security management practices.

We must caution, however, that this study has several caveats that may limit its generalizability. First, our findings are based on the data sample from a population with a unique Eastern culture where the concept of following rules and policies may be quite different from Western cultures. Culture has been found to significantly influence individual behavior in numerous studies.¹⁴ Second, the neutral wording used in scenarios of the survey could introduce unintended bias against deterrence in some respondents. Finally, the small number of organizations where the surveys were administered could bias the data as well. An interesting follow-up would be to replicate this study in multiple countries with various cultures using random samples that cover a large number organizations and industries. **C**

References

- Acquisti, A. and Gross, R. Imagined communities: Awareness, information sharing, and privacy on the Facebook. In *Proceedings of the 6th Workshop on Privacy Enhancing Technologies* (Cambridge, U.K., June 28–30, 2006).
- Anderson, R., Böhme, R., Clayton, R., and Moore, T. Security economics and European policy. In *Proceedings of the Workshop on Economics of Information Security* (New Haven, CT, 2008).
- Anderson, J.C., and Gerbing, S.W. Structural equation modeling in practice: A review and recommended two-step approach. *Psychological Bulletin* 103, 3 (1988), 411–423.
- Bachman, R., Paternoster, R., and Ward, S. The rationality of sexual offending: Testing a deterrence/rational choice conception of sexual assault. *Law & Society Review* 26, 2 (1992), 343–372.
- Becker, G. Crime and punishment: An economic approach. *Journal of Political Economy* 76, (1968), 169–217.
- Cable, D.M. and Judge, T.A. Person–organization fit, job choice decisions, and organizational entry. *Organizational Behavior and Human Decision Processes* 67, 3 (1996), 294–311.
- Cornish, D.B. and Clarke, R.V. *The Reasoning Criminal: Rational Choice Perspectives on Offending*. Springer-Verlag, New York, NY, 1986.
- D'Arcy, J., Havav, A., and Galletta, D. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20, 1 (2009), 79–98.
- Debatin, B., Lovejoy, J.P., Horn, A.K., and Hughes, B.N. Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication* 15, 1 (2009), 83–108.
- Dinev, T. and Hu, Q. The centrality of awareness in the formation of user behavioral intentions towards preventive technologies in the context of voluntary use. *Journal of the Association for Information Systems* 8, 7 (2007), 386–408.
- Ernst & Young. *Global Information Security Survey* (2008); <http://www.ey.com>.
- Gettfredson, M. and Hirschi, T. *A General Theory of Crime*. Stanford University Press, Stanford, CA, 1990.
- Gibbs, J. P. Crime, Punishment, and Deterrence. Elsevier, New York, NY, 1975.
- Hofstede, G. *Cultures and Organizations: Software of the Mind*. McGraw-Hill, New York, NY, 1991.
- Hulland, J. Use of partial least squares (PLS) in strategic management research: A review of four recent studies. *Strategic Management Journal* 20 (1999), 195–204.
- Lewis, M. *Shame: The Exposed Self*. Macmillan, New York, NY, 1992.
- Mercuri, R.T. Analyzing security costs. *Commun. ACM* 46, 6 (June 2003), 15–18.
- Nagin, D.S. and Paternoster, R. Enduring individual differences and rational choice theories of crime. *Law & Society Review* 27, 3 (1993), 467–496.
- Paternoster, R. and Simpson, S. Sanction threats and appeals to morality: Testing a rational choice model of corporate crime. *Law & Society Review* 30, 3 (1996) 549–583.
- Paternoster, R., Saltzman, L.E., Waldo, G.P., and Chiricos, T.G. Perceived risk and social control: Do sanctions really deter? *Law & Society Review* 17, 3 (1983), 457–480.
- Piquero, A. and Tibbetts, S. Specifying the direct and indirect effects of low self-control and situational factors in offenders' decision making: Toward a more complete model of rational offending. *Justice Quarterly* 13, 3 (1996), 481–510.
- Richardson, R. CSI Computer Crime & Security Survey (2008); <http://www.cse.msstate.edu/~cse6243/readings/CSISurvey2008.pdf>
- Ringle, C.M., Wende, S., and Will, A. SmartPLS, 2.0 (beta), University of Hamburg, Hamburg, Germany, 2005; <http://www.smartpls.de/>
- Simon, H. Bounded rationality in social science: Today and tomorrow. *Mind & Society* 1, 1 (2000), 25–39.
- Siponen, M. and Vance, A. Neutralization: New insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34, 2 (2010).
- Straub, D.W. and Welke, R.J. Coping with systems risk: Security planning models for management decision making. *MIS Quarterly* 22, 4 (1998), 441–469.
- Tittle, C. R. *Sanctions and Social Deviance: The Question of Deterrence*. Praeger, New York, NY, 1980.
- Tibbetts, S.G. and Gibson, C.L. Individual propensities and rational decision-making: Recent findings and promising approaches. In *Rational Choice and Criminal Behavior: Recent Research and Future Challenges*. A. R. Piquero and S. G. Tibbetts, eds. Routledge, New York, NY, 3–24.
- Tunnell, K. Choosing crime: Close your eyes and take your choices. *Justice Quarterly* 7, 4 (1990), 673–690.
- Warkentin, M. and Willison, R. Behavioral and policy issues in information systems security: The insider threat. *European Journal of Information Systems* 18 (2009), 101–105.

Qing Hu (qinghu@iastate.edu) is a professor and chair of the Department of Supply Chain and Information Systems at Iowa State University's College of Business, Ames, IA.

Zhengchuan Xu (zcxu@fudan.edu.cn) is an associate professor in the Department of Information Management and Information Systems at Fudan University's School of Management, Shanghai, China.

Tamara Dinev (tdinev@fau.edu) is an associate professor in the Department of Information Technology and Operations Management at Florida Atlantic University's College of Business, Boca Raton, FL.

Hong Ling (hling@fudan.edu.cn) is a professor and chair of the Department of Information Management and Information Systems at Fudan University's School of Management, Shanghai, China.