Online Appendix: A summary of prior studies on employee noncompliance behavior

The table below provides a summary of previous studies on employee noncompliance behavior, with a particular focus on research based on Deterrence Theory. The studies included in the table were selected based on our search on Web of Science using the keywords "employee compliance" and "deterrence" and covering the years from 2000 to 2022. This search yielded 65 journal publications. We excluded papers not written in English (e.g., Korean) (n=3). Additionally, we excluded non-empirical studies, such as narrative literature reviews and research commentaries, as they do not provide direct empirical evidence regarding the effect of deterrence on employee noncompliance (n=9). It is worth noting that none of the excluded studies examined the longitudinal effect of deterrence. Consequently, 53 publications remain. The table below summarizes these studies, detailing their main findings, research methods, data used, and research questions (RQ) addressed.

RQ1: Are deterrence-based controls effective in reducing employees' noncompliance behavior?

RQ2: Can the effect on employees' noncompliance behavior be sustained?

RQ3: What are the side effects of deterrence-based controls on employees' behaviors?

RQ4: Can the side effects be sustained?

Authors		Findings	Research Method	Data	Research Question(s) Addressed			
					RQ1	RQ2	RQ3	RQ4
1	Alshare et al. (2018)	Sanction severity and sanction celerity are significant predictors of violations of information security measures.	Cross-sectional survey	Self-reported data	√			
2	Aurigemma and Mattson (2017)	The effect of sanctions on employees' information security policy (ISP) compliance intention is fully mediated by their attitude towards the compliance. The sanction effects on the attitude can be biased by the past experience of punishment.	Cross-sectional survey	Self-reported data	√			

3	Chen et al. (2012)	The level of punishment for not complying with security policies is positively associated with the intention to comply with security policies. The level of reward for complying with security policies is positively associated with the intention to comply with security policies.	Scenario-based experiment	Self-reported data	√			
4	Chen et al. (2018)	Sanction severity has no direct effect on information security policy (ISP) compliance intention, self-efficacy of compliance and perceived descriptive norm mediate the relationship between sanction severity and ISP compliance intention.	Cross-sectional survey	Self-reported data	√			
5	Cheng et al. (2014)	Perceived detection certainty is found to have a negative effect on personal use of the Internet, while the effect of perceived sanction severity on personal use of the Internet is not significant.	Cross-sectional survey	Self-reported data	√			
6	Cram et al. (2019)	The effect sizes of detection certainty and punishment severity on employees' security policy compliance/violation are medium, that is, the effect sizes are between 0.30 and 0.50.	Meta-analysis	Existing literature findings	√			
7	D'Arcy and Hovav (2009)	The results suggest that computer savvy individuals are less deterred by SETA (security education, training, and awareness) programs and computer monitoring. These countermeasures are also less influential on employees who spend more working days outside the office.	Cross-sectional survey	Self-reported data	√			
8	D'Arcy and	Perceived computer monitoring is positively associated with average daily attitude toward	Experience	Self-reported	√			

	Lowry (2019)	information security policy compliance.	Sampling Survey	data				
9	D'Arcy et al. (2009)	User awareness of computer monitoring is positively associated with perceived certainty of sanctions and perceived severity of sanctions. Perceived severity of sanctions is negatively related to IS misuse intentions.	Cross-sectional survey	Self-reported data	√			
10	D'Arcy and Devaraj (2012)	The results suggest that a predisposition toward the need for social approval and moral beliefs regarding the behavior are key determinants of technology misuse. Threat of formal sanctions has both direct and indirect influences on technology misuse intention. Employees who spend more working days away from the office (i.e., "virtual" mode are more inclined to misuse their organization's technology resources.	Cross-sectional survey	Self-reported data	√			
11	Foth (2016)	Detection certainty is positively associated with intention to comply with data protection regulations. The effect of punishment severity on employees' intention to comply is not significant.	Cross-sectional survey	Self-reported data	√			
12	Glassman et al. (2015)	Among the three modules (blocking module, confirmation module and quota module) of the Internet filtering system, the confirmation module is the most effective one to reduce cyberloafing.	Econometrics model	Archival data	√			
13	Guo and Yuan (2012)	Personal self-sanctions and workgroup sanctions have significant deterrent effects on employee security violations, but that the effect of organizational sanctions becomes insignificant when the other two types of sanctions are taken	Scenario-based survey	Self-reported data	√			

		into account.						
14	Henle et al. (2009)	Employees are less likely to cyberloaf if the policy includes periodic monitoring.	Scenario-based (lab) experiment + Survey	Self-reported data	√			
15	Hensel and Kacprzak (2021)	Punishing the violators of organizational policy affect both the punished and unpunished employees. The effect was maintained for three months until the end of the dataset.	Field quasi-experiment (no control group)	Archival data	√	√		
16	Herath and Rao (2009a)	Certainty of detection is found to be positively related to security policy compliance intentions. Surprisingly, severity of punishment is found to have a negative effect on security behavior intentions. The effects of the two constructs are examined along with social pressures to comply and perceived effectiveness of security policies.	Cross-sectional survey	Self-reported data	√			
17	Herath and Rao (2009b)	Detection certainty is positively associated with security policy compliance intentions, and punishment severity is negatively associated with security policy compliance intentions. The effects of the two constructs are examined along with social norms (including subjective norm and descriptive norm), security policy attitude, self-efficacy, and organizational commitment.	Cross-sectional survey	Self-reported data	√			
18	Herath et al. (2018)	Punishment certainty and celerity (but not sanction severity) are instrumental toward reducing moral disengagement in the context of security policy compliance. Security education, training and awareness (SEAT) programs are	Cross-sectional survey	Self-reported data	√			

		useful to promote security policy awareness.						
19	Hovav and D'Arcy (2012)	Formal sanctions (including perceived certainty and severity of sanctions) are negatively related with IS misuse intention. The effect is generally stronger for U.S. individuals than Korean individuals. The effect of moral beliefs on IS misuse intention are both significant for U.S and Korean individuals, and the effect sizes are not significantly different across the two samples.	Cross-sectional survey	Self-reported data	√			
20	Ifinedo (2016)	Top management support and beliefs, sanction severity, and cost–benefit analysis significantly influenced employees' information systems security policy compliance intention.	Cross-sectional survey	Self-reported data	√			
21	Jaeger et al. (2021)	Information security policy compliance of inclined employees (i.e., those with a positive attitude) is mainly driven by their personal norms and not by perceptions of formal or informal sanctions. The disinclined compliers (i.e., those with a negative attitude who comply nevertheless) are deterrable. However, for disinclined compliers, the deterrence effect is predominantly exerted through punishment severity rather than punishment certainty. Moreover, the deterrence effect of informal sanctions appeared to play an important role in the compliance of disinclined compliers.	Cross-sectional survey	Self-reported data	√			
22	Johnston et al. (2016)	The negative effects of sanction severity and certainty on information security policy violation are more salient for individuals whose	Factorial survey	Self-reported	√			

		personalities favor Stability characteristics.		data				
23	Johnston et al. (2015)	The certainty and severity of informal (but not formal) sanctions are positively related with information security policy compliance intentions.	Scenario-based survey	Self-reported data	√			
24	Khansa et al. 2018	Technological interventions (e.g., internet monitoring) are effective at controlling cyberloafing, albeit at the expense of employee loyalty.	Scenario-based experiment	Self-reported data	√		√	
25	Khansa et al. 2017	The announcement of monitoring may change the relationship between cyberloafing and its antecedents. Before the announcement, employees' intentions to cyberloaf were mostly influenced by their past tendencies to cyberloaf and by others' cyberloafing, but their neutralization and perceived risk played no significant role. However, the impacts of individuals' neutralization and perceived risk on their cyberloafing became significant after the announcement.	Scenario-based experiment	Self-reported data	√			
26	Kuo et al. (2017)	Punishment certainty and detection certainty significantly reduced nurses' intentions to violate established electronic medical records (EMR) privacy policy. The effect of punishment severity was not significant.	Cross-sectional survey	Self-reported data	√			
27	Li et al. (2010)	Perceived detection probability (or sanction certainty) is positively related to security policy compliance intention. Perceived sanction severity is a significant deterrence mechanism only for	Cross-sectional survey	Self-reported data	√			

		employees with very low personal norms against internet abuse. For those with moderate to high personal norms, perceiving harsh sanctions not only failed to increase but reduced their compliance intension.						
28	Li et al. (2014)	The deterrence effect of formal sanctions is largely exerted through sanction certainty rather than sanction severity. Self-regulatory approach is more effective than the sanction-based command-and-control approach in promoting employees' internet use policy compliance.	Cross-sectional survey	Self-reported data	√			
29	Li et al. (2021)	There are situational differences in the deterrence effect of formal sanctions on information security policy violation intention. The effects of both sanction severity and sanction certainty are negligible in the personal internet use at work scenario; even if they do get caught, employees likely do not expect significant sanctions in response to this very common workplace behavior.	Scenario-based survey	Self-reported data	√			
30	Liao et al. (2009)	There is no support for the influence of punishment severity and punishment certainty on employee intention to misuse Internet.	Cross-sectional survey	Self-reported data	√			
31	Liu et al. (2022)	Punishment expectancy positively affects employee information systems security (ISP) compliance. Compared with committed employees, punishment expectancy has stronger impacts on low-commitment employees' ISP compliance. Punishment expectancy exerts a	Cross-sectional survey	Self-reported data	√			

		stronger effect on females' ISP compliance than it does on males.						
32	Lowry et al. (2015)	The deterrence theory (DT)-based constructs of sanction severity, certainty, and celerity have no significant influence on reactive computer abuse.	Cross-sectional survey	Self-reported data	√			
33	Malimage et al. (2020)	Certainty and celerity associated with deterrent sanctions increase compliance intentions related to modified information security policies.	Cross-sectional survey	Self-reported data	√			
34	Merhi and Ahluwalia (2019)	Punishment severity increases descriptive norms of information systems security (ISS) compliance, certainty of detection increases both descriptive norms and moral norms of ISS compliance. The two types of norms, in turn, decrease employees' resistance to ISS policy.	Cross-sectional survey	Self-reported data	√			
35	Moody et al. (2018)	The relationship between punishment and information security policy compliance intention is not significant.	Cross-sectional survey	Self-reported data	√			
36	Peace et al. (2003)	Punishment severity and certainty are found to have direct (and negative) effects on individuals' attitude toward noncompliance behavior in terms of software piracy. Punishment certainty has a significant effect on perceived behavioral control, which is a significant precursor to the intention to illegally copy software.	Cross-sectional survey	Self-reported data	√			
37	Posey et al. (2011)	Computer monitoring is found to increase internal computer abuse but not antisocial behaviors.	Cross-sectional survey	Self-reported data	√		√	

38	Raddatz et al. (2020)	Perceived sanction severity and certainty significantly influence intention to comply with computer usage policies. Awareness of being monitored is found to significantly impact penalties. Penalties may be effective only to the extent that organizations can detect employees' deviant behavior through managerial controls, such as computer monitoring.	Scenario-based experiment	Self-reported data	√			
39	Rahimnia and Mazidi (2015)	Organizational controls are only negatively related to other work loafing behaviors beyond cyberloafing (but self-control is negatively related to both cyberloafing and non-cyber loafing behaviors).	Cross-sectional survey	Self-reported data	√			
40	Rajab and Eydgahi (2019)	Little support is found for the Deterrence Theory in explaining the variance of higher education staff's intentions to comply with information security policies.	Cross-sectional survey	Self-reported data	√			
41	Sarkar et al. 2020	Professional subcultures moderate the effects of perceived certainty and severity of sanctions on information security policy violation intention.	Interview, Cross-sectional survey, Field observation	Observation data + Self-reported data	√			
42	Shahbaznezhad et al. (2021)	Detective countermeasures (e.g., monitoring capability) negatively affect employees' intention toward clicking on a phishing e-mail.	Cross-sectional survey	Self-reported data	√			
43	Silic et al. (2017)	Formal sanctions, informal sanctions, and shame did not have any deterring effect on shadow IT intention. Shame is influenced by informal	Cross-sectional survey	Self-reported data	√			

		sanctions but not formal sanctions.						
44	Siponen and Vance (2010)	The effects of formal and informal sanctions on employees' intention to violate information security policy are not significant when neutralization is included in the model.	Cross-sectional survey	Self-reported data	√			
45	Son (2011)	Neither of the coefficients on the paths from deterrent certainty and severity to employees' compliance with ISSP is statistically significant when the two variables (perceived legitimacy, perceived value congruence) rooted in the intrinsic motivation model are already in place.	Cross-sectional survey	Self-reported data	√			
46	Trinkle et al. (2014)	The presence of a social networking policy, logging awareness, and monitoring practices reduced participants' likelihood of playing online social networking games on company-owned computers.	Scenario-based experiment	Self-reported data	√			
47	Trinkle et al. (2021)	Sanctions play an important role in reducing employees' intentions to violate policy but employees might seek to rationalize their unethical behavior by denying responsibility for their actions. Messages heightening the awareness and perceptions of the certainty and severity of organizational punishment are likely to attenuate such deviant behaviors.	Scenario-based factorial survey	Self-reported data	√			
48	Ugrin and Pearson (2013)	Individually, threats termination and detection mechanisms are effective against activities like viewing pornography, managing personal finances and personal shopping, but must be coupled	Cross-sectional survey	Self-reported data	√			

		together and actively enforced to dissuade activities like personal e-mailing and social networking.						
49	Vance and Siponen (2012)	The effects of informal sanctions, moral beliefs, and perceived benefits convincingly explain employee IS security policy violations, while the effect of formal sanctions is insignificant	Scenario-based survey	Self-reported data	√			
50	Wang and Xu (2021)	Perceived deterrent certainty (but not severity) had a positive effect on information security policy compliance intention.	Cross-sectional survey	Self-reported data	√			
51	Xu et al. (2020)	Employees who experienced anger are more likely to commit computer-related deviant behavior mediated by perceived informal sanctions. Employees who experienced fear are less likely to commit computer-related deviant behavior mediated by perceived formal and informal sanctions.	Scenario-based survey	Self-reported data	√			
52	Zheng et al. (2020)	Authoritarian leadership thwarts employees' interpersonal deviance behavior when (1) leaders send clear signals of potential punishments of non-compliance by showing low leader benevolence, and (2) employees are highly dependent on the leaders for important work resources.	Cross-sectional survey	Self-reported data	√			
53	Zoghbi-Manrique-de-Lara and Olivares-Mesa	Monitoring is only effective to deter cyberloafing when combined with sanctions.	Cross-sectional survey	Self-reported data	√			

	(2010)							

References

Alshare KA, Lane PL, Lane MR (2018) Information Security Policy Compliance: A Higher Education Case Study. *Information & Computer Security* 26(1), 91-108.

Aurigemma S, Mattson T (2017) Deterrence and punishment experience impacts on ISP compliance attitudes. *Information & Computer Security*, *25*(4), 421-436.

Chen Y, Ramamurthy K, Wen KW (2012) Organizations' information security policy compliance: Stick or carrot approach?. *Journal of Management Information Systems*, *29*(3), 157-188.

Chen X, Wu D, Chen L, Teng JKL (2018) Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management*, 55 (8), 1049-1060

Cheng L, Li W, Zhai Q, Smyth R (2014) Understanding personal use of the Internet at work: An integrated model of neutralization techniques and general deterrence theory. *Computers in Human Behavior* 38, 220-228.

Cram WA, D'Arcy J, Proudfoot JG (2019) Seeing the Forest and the Trees: A Meta-Analysis of the Antecedents to Information Security Policy Compliance. *MIS Quarterly* 43(2): 525-554.

D'Arcy J, Hovav A (2009) Does one size fit all? Examining the differential effects of IS security countermeasures. *Journal of Business Ethics* 89(1): 59-71.

D'Arcy J, Lowry PB (2019) Cognitive-affective drivers of employees' daily compliance with information security policies: A multilevel, longitudinal study. *Information Systems Journal* 29(1): 43-69.

D'Arcy J, Hovav A, Galletta D (2009) User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research* 20(1): 79-98.

D'Arcy J, Devaraj S (2012) Employee misuse of information technology resources: Testing a contemporary deterrence model. *Decision Sciences* 43(6): 1091-1124.

Foth M (2016) Factors influencing the intention to comply with data protection regulations in hospitals: based on gender differences in behavior and deterrence. *European Journal of Information Systems* 25(2): 91-109.

Glassman J, Prosch M, Shao BBM (2015) To monitor or not to monitor: Effectiveness of a cyberloafing countermeasure. *Information & Management* 52(2):170-182.

Guo KH, Yuan Y (2012) The effects of multilevel sanctions on information security violations: A mediating model. *Information & Management* 49(6): 320-326.

Henle CA, Kohut G, Booth R (2009) Designing electronic use policies to enhance employee perceptions of fairness and to reduce cyberloafing: An empirical test of justice theory. *Computers in Human Behavior* 25(4): 902-910.

Hensel PG, Kacprzak A (2021) Curbing cyberloafing: studying general and specific deterrence effects with field evidence. *European Journal of Information Systems* 30(2): 219-235.

Herath T, Rao HR (2009a) Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems* 47(2): 154-165.

Herath T, Rao HR (2009b) Protection motivation and deterrence: a framework for security policy compliance in organizations. *European Journal of Information Systems* 18(2): 106-125.

Herath T, Yim MS, D'Arcy J, Nam K, Rao HR (2018) Examining employee security violations: moral disengagement and its environmental influences. *Information Technology & People* 31 (6), 1135-1162.

Hovav A, D'Arcy J (2012) Applying an extended model of deterrence across cultures: An investigation of information systems misuse in the US and South Korea. *Information & Management* 49(2): 99-110.

Ifinedo P (2016). Critical times for organizations: What should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management*, 33(1): 30-41.

Jaeger L, Eckhardt A, Kroenung J (2021) The role of deterrability for the effect of multilevel sanctions on information security policy compliance: Results of a multigroup analysis. *Information & Management* 58(3): 103318.

Johnston AC, Warkentin M, McBride M, Carter L (2016) Dispositional and situational factors: influences on information security policy violations. *European Journal of Information Systems* 25(3): 231-251.

Johnston AC, Warkentin M, Siponen M (2015) An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. *MIS Quarterly* 39(1): 113-134.

Khansa L, Barkhi R, Ray S, Davis Z (2018) Cyberloafing in the workplace: mitigation tactics and their impact on individuals' behavior. *Information Technology and Management* 19(4):197-215.

Khansa L, Kuem J, Siponen M, Kim SS (2017) To cyberloaf or not to cyberloaf: The impact of the announcement of formal organizational controls. *Journal of Management Information Systems* 34(1):141-176.

Kuo, KM, Talley PC, Hung MC, Chen YL (2017) A Deterrence Approach to Regulate Nurses' Compliance with Electronic Medical Records Privacy Policy. *Journal of Medical Systems* 41(12): 1-10.

Li H, Zhang J, Sarathy R (2010) Understanding compliance with internet use policy from the perspective of rational choice theory. *Decision Support Systems* 48(4): 635-645.

Li H, Sarathy R, Zhang J, Luo X (2014) Exploring the effects of organizational justice, personal ethics and sanction on internet use policy compliance. *Information Systems Journal*, 24(6): 479-502.

Li H, Luo XR, Chen Y (2021) Understanding information security policy violation from a situational action perspective. *Journal of the Association for Information Systems* 22(3): 739-772.

Liao Q, Gurung A, Luo X, Li L (2009) Workplace management and employee misuse: does punishment matter? *Journal of Computer Information Systems*, 50(2): 49-59.

Liu C, Liang H, Wang N, Xue Y (2022) Ensuring employees' information security policy compliance by carrot and stick: the moderating roles of organizational commitment and gender, *Information Technology & People*, 35(2): 802-834.

Lowry PB, Moody GD (2015) Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organizational information security policies. *Information Systems Journal* 25(5): 433-463.

Malimage K, Raddatz N, Trinkle BS, Crossler RE, Baaske R (2020) Impact of deterrence and inertia on information security policy changes. *Journal of Information Systems*, *34*(1), 123-134.

Merhi MI, Ahluwalia P (2019) Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior* 92: 37-46.

Moody GD, Siponen M, Pahnila S (2018) Toward a unified model of information security policy compliance. *MIS Quarterly* 42(1):285-311.

Peace AG, Galletta DF, Thong JY (2003) Software piracy in the workplace: A model and empirical test. *Journal of Management Information Systems* 20(1): 153-177.

Posey C, Bennett B, Roberts T, Lowry PB (2011) When computer monitoring backfires: Invasion of privacy and organizational injustice as precursors to computer abuse. *Journal of Information System Security* 7(1): 24-47.

Raddatz NI, Marett K, Trinkle BS (2020). The impact of awareness of being monitored on computer usage policy compliance: An agency view. *Journal of Information Systems*, *34*(1), 135-149.

Rahimnia F, Mazidi ARK (2015) Functions of control mechanisms in mitigating workplace loafing; evidence from an Islamic society. *Computers in Human Behavior* 48: 671-681.

Rajab M, Eydgahi A (2019) Evaluating the explanatory power of theoretical frameworks on intention to comply with information security policies in higher education. *Computers & Security* 80: 211-223.

Sarkar S, Vance A, Ramesh B, Demestihas M, Wu DT (2020) The influence of professional subculture on information security policy violations: A field study in a healthcare context. *Information Systems Research* 31(4):1240-1259.

Shahbaznezhad H, Kolini F, Rashidirad M (2021) Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems* 61(6): 539-550.

Silic M, Barlow JB, Back A (2017) A new perspective on neutralization and deterrence: Predicting shadow IT usage. *Information & Management* 54(8): 1023-1037.

Siponen M, Vance A (2010) Neutralization: new insights into the problem of employee information systems security policy violations. *MIS Quarterly* 34(3):487-502.

Son JY (2011) Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. *Information & Management* 48(7): 296-302.

Trinkle BS, Crossler RE, Warkentin M (2014) I'm game, are you? Reducing real-world security threats by managing employee activity in online social networks. *Journal of Information Systems*, *28*(2), 307-327.

Trinkle BS, Warkentin M, Malimage K, Raddatz N (2021). High-risk deviant decisions: does neutralization still play a role?. *Journal of the Association for Information Systems*, *22*(3), 797-826.

Ugrin JC, Pearson JM (2013) The effects of sanctions and stigmas on cyberloafing. *Computers in Human Behavior* 29(3): 812-820.

Vance A, Siponen MT. (2012) IS security policy violations: A rational choice perspective. *Journal of Organizational and End User Computing*, *24*(1), 21-41.

Wang X, Xu J (2021). Deterrence and leadership factors: Which are important for information security policy compliance in the hotel industry. *Tourism Managemen* 84:104282.

Xu F, Luo XR, Hsu C (2020) Anger or fear? Effects of discrete emotions on employee's computer-related deviant behavior. *Information & Management*, 57, 103180.

Zheng Y, Huang X, Graham L, Redman T, Hu S (2020). Deterrence effects: The role of authoritarian leadership in controlling employee workplace deviance. *Management and Organization Review* 16(2): 377-404.

Zoghbi-Manrique-de-Lara P, Olivares-Mesa A (2010) Bringing cyber loafers back on the right track. *Industrial Management & Data Systems* 110(7): 1038-1053.