Bosses Behaving Badly: Managers Committing Computer Abuse

Completed paper

Laura Amo
State University of New York at Buffalo
lccasey@buffalo.edu

ABSTRACT

The zero-trust model for information security assumes that no network or person can be fully trusted, and it has been advocated for mitigation of insider threats. Managers, however, tend to be regularly entrusted with extensive access to organizational information and systems, creating more opportunity for insider behavior. I draw on theories of power and criminology to theorize that managers are more likely to engage in computer abuse behavior because they have greater opportunity/access due to having more legitimate power in the organization. In the present study (n = 437 working adults), I examine aspects of managerial status including level of management and number of supervisees and determine that both are positively related to computer abuse. I determine that managers are more likely to engage in computer abuse compared to non-managers, and that the more employees that a manager supervises, the more likely they are to engage in this deviant behavior. I then go on to establish a causal chain in the relationship between managerial status and computer abuse through managerial need for power; managers are more likely to have a strong need for power which is related to computer abuse. This work contributes to the research on insider threats, and has direct implications for practice.

Keywords

Insider threat, computer abuse behavior, managerial position, need for power

INTRODUCTION

Power is recognized as a “great motivator” but does it motivate bad behavior? More specifically, does power motivate insider behavior? Theories in white-collar crime and occupational fraud suggest that the answer is “yes.” For example, company owners and executives make up for nearly 20% of all business fraud cases according to the Association of Certified Fraud Examiners ([ACFE], 2018). Individuals with greater organizational power are more likely to engage in deviant work behavior and, therefore, are also part of the growing insider threat. Organizational insiders are employees who pose threats to an organizations’ technological assets and resources and these employees cost organizations millions annually (Ponemon, 2022). Although employees at all levels pose threats to organizational assets, I argue that managers and organizational leaders are uniquely positioned and psychologically poised to commit computer abuse and have the potential to cause significant damage to companies.

Herein, I introduce the concept of managerial computer abuse, defined as the misuse and abuse of technological resources and systems by organizational leaders, as an example of how legitimate power can motivate workplace deviance. Although the large body of research on organizational insiders has identified individual and organizational factors that contribute to computer abuse (e.g. Amo et al., 2022; Burns et al., 2022; D’Arcy & Devaraj, 2012; D’Arcy, Hovav, & Galleta 2009; D’Arcy & Hovav 2009; Lowry et al., 2015; Willison & Backhouse, 2006), managerial factors have been ostensibly overlooked. Studies of computer abuse and information security violation either do not consider management roles (e.g. Amo et al., 2022; Kim et al., 2016) or model variables associated with managerial status and employee level as a control (e.g. Burns et al., 2022; D’Arcy & Devaraj, 2012; Lowry et al., 2015; Xu et al., 2020).

To address growing threats to information security and insider computer abuse, there have been recent calls for zero-trust security architectures to be widely adopted, which is a model that assumes no person or network within an organization is trustworthy (see Buck et al. 2021). In practice, however, while zero-trust architectures are recommended and many companies indicate ongoing initiatives, this practice is still uncommon. As of February 2022, only about 21% of enterprises used zero trust architecture (VentureBeat 2022). Relevant to the present work, managers in particular tend to be granted broad access to organizational information and systems and enjoy elevated privileges (Kemp, 2015).

Building off work by Willison and Backhouse (2006), I draw on the criminology literature to hypothesize that managers will be more likely to engage in computer abuse. I integrate aspects from Gottschalk’s (2020) model of white-collar crime convenience and explore the extent to which status - in the form of managerial status, managerial level, and number of subordinate employees - predicts computer abuse behavior. I then integrate literature on power to examine how managerial need for power explains their propensity to engage in computer abuse.

In the present study, I address the following questions: Are managers more likely to engage in computer abuse? Does having more legitimate power (level of management, number of supervisees) predict computer abuse? Does psychological need for power explain the relationship between managerial status and computer abuse? Below, I provide a brief overview of the studies that have explored managerial status in relation to computer abuse, and then discuss theory on white collar crime and power before introducing my hypotheses. I then outline my methods, present my results, and discuss my findings.

OVERVIEW OF RELEVANT LITERATURE

Existing Research on Managerial Position and Computer Abuse Behavior

Overall, there has been very little research on the relationship between managerial position and computer abuse. Based on a review of over 30 studies on computer abuse intent and behavior spanning the past 35 years , only four studies included managerial status as a control variable (Burns et al. 2022; D'Arcy & Devaraj, 2012; Lowry et al. 2015; Xu et al. 2020). There has yet to be a direct theoretically-driven investigation of the relationship between managerial position and computer abuse. This is surprising, given that managers tend to have greater access and privilege to systems and networks in the organization and they are involved in information security policy creation and enforcement, granting them greater opportunity to commit computer abuse and better knowledge of policy loopholes. If managers are indeed more likely to engage in computer abuse, this is a unique type of insider threat that is currently overlooked and is relevant to new calls for zero-trust policies in organizations.

Criminological Perspectives on Computer Abuse

Although computer abuse studies have incorporated a number of criminological theories to understand computer abuse including techniques of neutralization (Siponen & Vance, 2010; Willison & Warkentin, 2013; Willison, Warkentin, & Johnston, 2018) and crime opportunity structures (e.g. Kim et al. 2015; Willison & Backhouse, 2006), white collar criminological theory is most relevant to managers and executives. White collar crimes are committed by institutions or individuals occupying a position with legitimate status and are crimes intended to gain financial advantage or maintain power and privilege (Freidrichs, 2020). According to a recent report on white-collar crime and insider threats (Black, Yeung & Yeung, 2023), white collar criminals tend to have positions of power in organizations, making this literature particularly relevant to the present study.

Gottschalk's theory of white-collar crime convenience (2022) recognizes that status in organizations lends itself to greater access and more opportunity to commit a crime. Specifically, status differences within an organization lead to variations in opportunity to commit a crime as well as expectations about certain privileges (Han et al. 2017; Gottschalk 2022). In other words, individuals with higher status (e.g. managers and leaders) have more opportunities to commit crimes and feel a sense of entitlement regarding criminal behavior. Moreover, white-collar criminals also typically have legitimate access to the resources to commit the respective crime (Kempa, 2010; Huisman & Erp 2013; Williams et al. 2019).

Applying this to the context of work technology, managers generally feel that they deserve greater access to technological resources (i.e. systems, networks, locations) and are often times given such broad access, or privileged identities (Kemp, 2015). From this perspective, managerial status may be associated with computer abuse simply because these employees are able to conveniently access technological systems and resources that they may otherwise not be able to access.

Organizational Power and Power Seeking

At the same time, organizational managers also have power which may also be related to deviant work behavior such as computer abuse. The primary source of power in organizations is legitimate power (formal or bureaucratic), or the power assigned to a person based on job designation or title, and this type of power is allocated according to rank level within the organization (French & Raven, 1959). Power helps control individuals, departments, and organizations.

According to human motivation theory (or express motives theory), every person has one of three main driving motivators: the need for achievement, the need for affiliation, and the need for power (McClelland, 1965). Power motive, or the need for power, is characterized by a desire to impact or control others (McClelland, 1965). Managers tend to have high need for power, and, according to some research, managers aligned with a strong need for power (as opposed to those with a high need for achievement or high need for affiliation) are the “best” managers (McClelland & Burnham, 2003). Managers, being in a position of authority and high position, are also more likely to have a high need for power. Central to this study, power motive is associated with counterproductive work behavior (Cortina et al. 2001; Molho 2019).

RESEARCH MODEL AND HYPOTHESES

Altogether, the criminological research and research on power theory suggests that managers, due to having legitimate power, status, and enhanced access to resources, may be more likely to engage in white-collar crimes such as computer abuse. Combining these perspectives, I present my hypotheses below.

First, managers in general have more legitimate power and may therefore have more knowledge about the control systems and mechanisms in place to thwart insider attacks. This grants managers an advantage and greater opportunity to commit computer abuse. There is research confirming that persons in high-powered positions are more likely to engage in white-collar crimes such as financial statement fraud (ACFE 2018). For example, according to a 2018 report on 2,690 cases of fraudulent business practices from 2016 - 2017, 65% of all fraud incidents were conducted by owners or executives. Aligned with opportunistic theory in criminology (Gattschalk 2006) and work in computer abuse positioning computer abuse from an opportunistic perspective (Kim et al. 2016; Willison & Backhouse 2006), I posit that because managers overall will engage in more computer abuse (H1A):

Hypothesis 1: Managers are more likely to engage in computer abuse compared to non-managers.

I also posit that managerial level has a positive linear relationship with computer abuse such that managers with greater managerial status are even more likely to engage in computer abuse behavior. Managers with higher status have greater legitimate power, and tend to expect more privileges (Han et al. 2017; Gottschalk 2022). As Gottschalk (2022) points out, high-level executives also have more ability to cover up crimes, making them more likely to engage in white collar criminal activity. The corporate fraud literature supports a strong link between level of authority and deviant work behavior, as reports consistently demonstrate a linear relationship between level of authority and fraud loss; the greater the level of perpetrator's authority, the greater the fraud losses (ACFE, 2014, 2020).

Extending this to the computer abuse context, and beyond comparisons between non-managers and managers as in H1, I also hypothesize that computer abuse behavior grows as managerial status increases. Managerial status can be conveyed in different ways, the first of which is in terms of managerial level; low-level managers, for example, have relatively less status compared to high-level managers. Managerial status can also be conveyed in terms of span of control, or the number of subordinate employees (Gartner 2023). Both forms of managerial status serve as an external validation of power, reinforcing managers' self-importance and perception of control which, I argue, leads to more computer abuse. I hypothesize that as management level increases (i.e. from no managerial status to low-level management to mid-level management to upper-level management), computer abuse behavior likewise increases at each step up the managerial ladder (H2A) and that as managerial span of control increases (i.e. more subordinate employees) so too does computer abuse behavior (H2B):

Hypothesis 2A: The higher the level of management, the more likely an employee is to engage in computer abuse.

Hypothesis 2B: The more employees that a manager is responsible for overseeing, the more likely they are to engage in computer abuse.

Lastly, I hypothesize that the effects between managerial factors (status, level, and span of control) and computer abuse are mediated by power motive. Exploration of mediated effects is incredibly important in research, as it provides enhanced insight into causality and explicates how the effect is transmitted from the independent variable to the outcome (MacKinnon et al., 2007). Towards developing a more detailed perspective on the causal chain in the manager-computer abuse relationship, in my last hypothesis I explore the extent to which direct effects outlined in my preceding hypotheses (i.e. H1, H2A, H2B) are explained by managerial power motive.

Overall, managers are likely to have higher power motive (McClelland, 1965). Individuals who work to gain managerial positions are driven by the need for power, explaining their pursuit and attainment of managerial positions. Power motive is associated with aggression (Królewiak, 2017), and has been linked with counterproductive work behavior (Cortina et al. 2001; Molho 2019). As such, I posit that the will be associated with more computer abuse behavior

Hypothesis 3: The effects that managerial position, management level, and managerial span of control have on computer abuse are mediated by power motive.

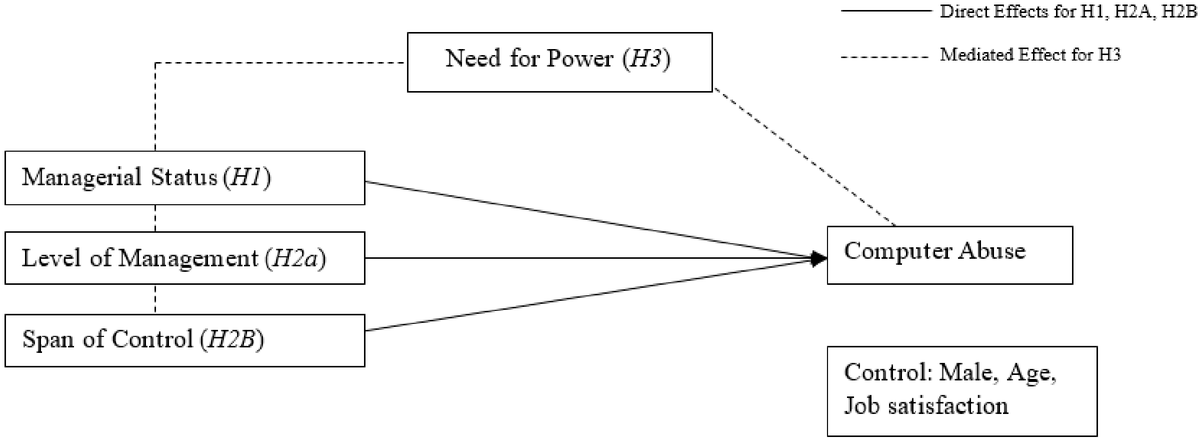

Figure 1. Research Model

METHODS

Overview

I conducted a field study with participants recruited by a survey panel company (Cint™) in October 2022. Participants were asked to complete a survey online and needed to pass three attention checks in order to be included in the final sample. Of the 734 respondents, 437 passed all three attention checks in the survey. The participants had individual agreements with the survey company regarding compensation for surveys so compensation varied across participants.

Sample

The final sample was comprised of 437 participants. About 38% of the respondents were male, 50% were managers, and the average age was 44.8. All descriptive statistics and correlations from the models are reported in Table 1. Additional demographic information that was not included in statistical models included educational level, tenure, race, company size, and age of company. The distribution of educational level of participants was such that 28% had a high school diploma, 19% of the respondents had an associate's degree, 33% of the respondents had a bachelor's degree, and

19% had a graduate degree. In terms of tenure, about 45% of the participants had 5 years or less at their current job, 12.5% had between 5 and 7 years, 12.5% had between 7 and 10 years, and 30% had more than 10 years at their current job. About 72% of the participants were Caucasian, 11% were Black, 4.5% were Asian, 10% were Hispanic, and 2.5% indicated “Other.” Company size distribution was such that about 17.5% had under 20 employees, 16.5% had between 20 and 100 employees, 20% had between 101 and 500 employees and 46% worked in companies with over 500 employees. Company age varied from 6.5% of companies between less than 5 years old, about 30% working at companies between 5 and 20 years old, 48.5% working at companies older than 20 years but less than 100, and about 15% of participants working at companies that were over 100 years old.

Measures

Participants’ gender, age, and managerial status were asked directly and correspond to the items for male (1 = “Yes”), age (continuous), and manager (1 = “Yes”). The job satisfaction scale was from Cammann et al., (1983) with α = .916. If respondents indicated that they were managers, follow-up questions about the number of employees that they managed and the level of management were asked. Specifically, participants were asked to select from the following list with regard to their managerial level: 1 = “First-line management (e.g. shift supervisor; managers that most employees interact with on a daily basis,” 2 = “Middle management (e.g. heading a specific department, assisting first-line managers),” and 3 = “Upper management (E.g. CEO, COO, vice-president).” To measure span of control, participants were asked to indicate the number of employees they were responsible for managing by selecting from the following list: 1 = “between 1 and 5 employees,” 2 = “between 6 and 19 employees,” 3 = “between 20 and 99 employees,” 4 = “100 or more employees.” For non-managers, managerial level and span of control were coded as

0. Computer abuse was measured with the 9-item reactive computer abuse scale from Lowry et al. (2015) with α = .849, and the need for power was measured by the Personalized Need for Power scale in Moon et al. (2021) with α = .802.

Analysis

The linear regression models were run in SPSS (IBM, 2016). Due to skewness of the dependent variable (computer abuse), the natural log of computer abuse was used as the dependent variable. The model with control variables was run first (Table 2), and then the separate models for the management factors were run (Model 1 in Table 3, Table 4, and Table 5). Due to the collinearity of the management variables, these were run in separate models. The mediation models were run in the SPSS add-on PROCESS; in the PROCESS macro, indirect effects are estimated using bootstrapping methods (n = 10,000 samples) (see Hayes, 2013). The results for the mediation analysis of the effects of managerial status, management level, and span of control on computer abuse through power motive are provided in Model 2 in Tables 3, 4, and 5, respectively.

RESULTS

The findings from the study support Hypothesis 1. As shown in Table 4, managerial position was associated with the computer abuse behavior after controlling for gender, age, and job satisfaction, B = .12, p < .001 in support of H1. Comparing the R2 values from Table 2 to the R2 values in Model 1 of Table 3, managerial position explained an additional 1% in the variance in computer abuse. Hypothesis 2 was also supported. Management level was significantly associated with computer abuse, B = .03, p < .01 and explained an additional 1% of the variance in the outcome (see Model 1, Table 4) in support of H2A. The results also supported H2B, as shown in Table 5. Managerial span of control was also associated with computer abuse, B = .03, p < .01, and explained nearly 2% additional variance in computer abuse behavior.

Findings also supported Hypothesis 3. The effects of each of the managerial variables on computer abuse were mediated by power motive. The indirect effect of managerial status on computer abuse via power motive was .0215, 95% CI [.007, .0414], as shown in Table 3. Managerial status predicted power motive, B = .29, p < .01, which predicted computer abuse, B = .07, p < .001. Similarly, as shown in Table 4 (Model 2), management level predicted power motive, B = .14, p < .001, which predicted computer abuse, B = .07, p < .001. Overall, the indirect effect was B = .0103, 95% CI [.0033, .0199]. Finally, span of control predicted power motive, B = .15, p < .001 which again predicted computer abuse, B = .07, p < .001. As shown in Table 5, the indirect effect was estimated at B = .0103, 95% CI [.0033, .0205].

The mediation effect may be considered a partial one, as the direct effects of the managerial variables remained significantly related to computer abuse in each of the different regression models. In other words, power motive explained some but not all of the effects that manager-related factors had on computer abuse.

		Min	Max	Mean	SD	1	2	3	4	5	6	7	8
1	Male	0	1	.382	.48	1							
2	Age	20	65	44.84	10.9	-.01	1						
3	Manager	0	1	.52	.50	.14	-.09	1					
4	Need for Power	1	6.44	2.51	.97	.16***	-.17***	.17***	1				
5	Job satisfaction	1	7.00	5.45	1.40	-.03	-.03	.09*	-.20***	1			
6	Subordinates	0	4	.99	1.16	.20***	-.11*	.82***	.21***	.06	1		
7	Management level	0	3	.10	1.16	.15***	-.05	.88***	.17***	.13**	.77***	1	
8	Computer abuse	0	1.49	.23	.28	.23***	-.12**	.143**	.32***	-.12**	.19***	.15***	1

Notes: ^ *p* <.1, * *p* <.05, ** *p* < .01, *** *p* < .001.

Table 1. Descriptive Statistics and Correlations

	B	SE	t
Male	.13	.03	4.83***
Age	-.00	.00	-2.66***
Job satisfaction	-.02	.01	-2.47**
R^2_{ADJ}			.073

Table 2. Control Variables Predicting Computer Abuse (n = 437)

Model	Dependent Variable		B	SE	t-statistic	R^2	Indirect Effect
1	Computer Abuse	Male	.12	.03	4.46***	.084	.0215 [.007,.0414]
		Age	-.00	.00	-2.47*		
		Job satisfaction	-.03	.01	-2.69***		
		Manager	.06	.03	2.45**		
2	Power motive	Male	.25	.09	2.72**	.1135	
		Age	-.01	.00	-3.43***		
		Job satisfaction	-.15	.03	-4.69***		
		Manager	.29	.09	3.3***		
	Computer Abuse	Male	.10	.03	3.87***	.1487	
		Age	-.00	.00	-1.65*		
		Job satisfaction	-.01	.01	-1.53^		
		Manager	.04	.03	1.65*		
		Need for Power	.07	.01	5.32***		

Notes: ^ *p* <.1, * *p* <.05, ** *p* < .01, *** *p* < .001.

Table 3. The Relationship between Managerial Position and Computer Abuse Mediated by Need for Power (*n* = 437)

Model	Dependent Variable		B	SE	t-statistic	R^2	Indirect Effect
1	Computer Abuse	Male	.12	.03	4.41***	.087	.0103 [.0033,.0199]
		Age	-.00	.00	-2.67*		
		Job satisfaction	-.03	.01	-2.82***		
		Management Level	.03	.01	2.73**		
2	Power motive	Male	.25	.09	2.67**	.1165	
		Age	-.01	.00	-3.56***		
		Job satisfaction	-.15	.03	-4.85***		
		Management Level	.14	.04	3.5***		
	Computer Abuse	Male	.10	.03	3.84***	.1504	
		Age	-.00	.00	-1.72*		
		Job satisfaction	-.02	.01	-1.63^		
		Management Level	.02	.02	1.89*		
		Need for Power	.07	.01	5.26***		

Notes: ^ *p* <.1, * *p* <.05, ** *p* < .01, *** *p* < .001.

Table 4. The Relationship between Managerial Level and Computer Abuse Mediated by Need for Power (*n* = 437)

Model	Dependent Variable		B	SE	t-statistic	R^2	Indirect Effect
1	Computer Abuse	Male	.11	.03	4.21***	.09	.0103 [.0033,.0205]
		Age	-.00	.00	-2.69*		
		Job satisfaction	-.03	.01	-2.69***		
		Span of control	.03	.01	2.99**		
2	Power motive	Male	.23	.09	2.45**	.1196	
		Age	-.01	.00	-3.33***		
		Job satisfaction	-.15	.03	-4.68***		
		Span of control	.15	.04	3.73***		
	Computer Abuse	Male	.10	.03	3.69***	.1521	
		Age	-.00	.00	-1.59^		
		Job satisfaction	-.01	.01	-1.56^		
		Span of control	.02	.01	2.11*		
		Need for Power	.07	.01	5.20***		

Notes: ^ *p* <.1, * *p* <.05, ** *p* < .01, *** *p* < .001.

Table 5. The Relationship between Number of Subordinate Employees and Computer Abuse Mediated by Need for Power (*n* = 437)

CONCLUSION

As the costs of insider threat continue to increase, identification of these threats remains an important endeavor for scholars and practitioners. In the present study, I discovered that managers are significantly more likely than non-managers to engage in computer abuse (H1) and I also find that that this threat grows as management level (H2A) and span of managerial control increase (H2B). This is alarming for several reasons. Managers are in positions of organizational authority and they have legitimate access to sensitive data systems and information, which may make it easier for them to commit computer abuse. However, data privilege and access alone do not inevitably lead to commit computer abuse. Managers are also more likely to have a strong need for power, or power motive, which has shown to be related to counterproductive work behavior in past research (Cortina; Molho et al. 2019), and was also associated with computer abuse in the present study. In fact, my study shows that this need for power explains some of the relationship between managerial factors and computer abuse (H3), but not all of it. Even after controlling for power motive, variables related to management status in this study were still significantly related to computer abuse.

Practical Implications

As a means to help manage information security risk, there have been calls for zero-trust architecture, most notably by the President of the United States calling for federal zero trust architecture in all U.S. government systems by the end of 2024 (Young, 2022). However, there are ongoing challenges to implementation of zero trust (e.g. Buck et al. 2021) including employee perceptions of injustice (Gigamon 2020). Our data lends strong support for zero-trust policies. Managers are typically provided elevated privileges to technology and data systems, and the principle of least-privilege (POLP) is not generally extended to managers and executives (Legg, 2022; Kemp, 2015). As shown herein, managers and executives are more likely to engage in computer abuse which suggests that their elevated access to networks and systems may be putting companies at greater risk of insider behavior. If zero-trust architecture was implemented, managers' privileged access to systems would be minimized and this threat would theoretically be better managed.

Another implication of our research is the potential contagion effect of counterproductive work behavior such as computer abuse. Organizational research has suggested that counterproductive work behavior can spread within organizations (O'Boyle et al., 2011). If managers engage in computer abuse and it is observed by other employees, particularly among subordinates, this will establish informal norms that computer abuse is acceptable and likewise affect computer abuse among other employees in the organization.

Theoretical Implications

Findings from this study contribute to the theory on white collar crime, and specifically support aspects of Gottschalk's theory on white collar convenience crime (2022). This theory states that executive employees are afforded greater status and access, which is one explanation for their propensity to commit financial crime. Extending this theory to explain computer abuse, managers have greater access to data and technological systems, which is one potential reason why managers are significantly more likely to engage in computer abuse compared to non-managers. Similarly, managerial level was also associated with computer abuse in this study. As management level increased (and the associated status with that managerial level), computer abuse likewise increased. Status may also be established by way of span of control, or the number of employees that the manager is responsible for overseeing, which was also associated with computer abuse in this study.

Limitations and Future Research

As with all research, this study had limitations. One limitation was that network access was not directly addressed which is an important mediator to measure and test in future research. This will help provide information on whether managers indeed have elevated privilege, and if this is associated with computer abuse, and directly test this particular aspect of the white-collar convenience crime theory (Gottschalk, 2022). Future research may also determine if managerial computer abuse is exacerbated in certain work environments to determine when these privileged employees are most likely to pose harm to organizations.

ACKNOWLEDGEMENTS

I would like to thank the anonymous reviewers for their insightful feedback on this submission.

REFERENCES

Amo, L.C., Grijalva, E., Herath, T., Lemoine, J., and Rao, H.R. (2022). Technological entitlement: It's my technology and I'll (ab)use it how I want to. *MIS Quarterly, 46*(3), pp. 1395 – 1420.

Association of Certified Fraud Examiners (ACFE 2014). Report to the Nations®. 2014 Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Association of Certified Fraud Examiners (ACFE 2018). Report to the Nations®. 2018 Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Association of Certified Fraud Examiners (ACFE 2020). Report to the Nations®. 2020 Global Study on Occupational Fraud and Abuse. Association of Certified Fraud Examiners. https://www.acfe.com/fraud-resources/report-to-the-nations-archive

Black, M., Yeung, J., and Yeung, D. (2022). *Insider Threat and White-Collar Crime in Non-Government Organisations and Industries: A Literature Review*. Santa Monica, CA: RAND Corporation, 2022. https://www.rand.org/pubs/research_reports/RRA1507-1.html.

Buck, C., Olenberger, C., Shweizer, A., Völter, F., and Eymann, T. (2021). Never trust, always verify: A multivocal literature review on current knowledge and research gaps of zero-trust. *Computers and Security*, 110, (102436).

Burns, A. J., Roberts, T. L., Posey, C., Lowry, P. B., & Fuller, B. (2022). Going Beyond Deterrence: A Middle-Range Theory of Motives and Controls for Insider Computer Abuse. *Information Systems Research*, Online First.

Cammann, C., Fichman, M., Jenkins, G. D., & Klesh, J. (1983). Michigan organizational assessment questionnaire. In S. E. Seashore, E. E. Lawler, P. H. Mirvis, & C. Cammann (Eds.), *Assessing organizational change: A guide to methods, measures, and practices* (pp. 71-138). Wiley-Interscience.

Cortina, L. M., Magley, V. J., Williams, J. H., & Langhout, R. D. (2001). Incivility in the workplace: incidence and impact. *Journal of Occupational Health Psychology*, *6*(1), 64–80.

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

D'Arcy, J., & Hovav, A. (2009). Does One Size Fit All? Examining the Differential Effects of IS Security Countermeasures. *Journal of Business Ethics, 89*(S1), 59-71. doi:10.1007/s10551-008-9909-7

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. doi:10.1287/isre.1070.0160

French, J. R. P., Jr., & Raven, B. (1959). The bases of social power. In D. Cartwright (Ed.), *Studies in social power* (pp. 150–167). Univer. Michigan.

Friedrichs D. O. (2020). White collar crime: Definitional debates and the case for a typological approach. In Rorie M. L. (Ed.), *The handbook of white collar crime* (pp. 16–31). Hoboken, NJ: Wiley Blackwell.

Gartner (2023). Span of control. Retrieved from https://www.gartner.com/en/human-resources/glossary/span-of-control

Gigamon. (2020). *The IT & Security Landscape for 2020 and Beyond and the Role of Zero Trust.*
Gigamon. https://blog.gigamon.com/2020/09/28/the-it-security-landscape-for-2020-and-beyond-and-the-role-of-zero-trust/

Gottschalk, P. (2022). Trusted Chief Executives in Convenient White-Collar Crime. *Crime & Delinquency*, Online First, https://doi.org/10.1177/00111287221104737

Han, J., Shipilov, A. V., & Greve, H. R. (2017). Unequal bedfellows: Gender rolebased deference in multiplex ties between Korean business groups. *Academy of Management Journal*, *60*(4), 1531–1553.

Hayes, A. F. (2013). *Introduction to mediation, moderation, and conditional process analysis: A regression-based approach*. Guilford Press.

Huisman & van Erp (2013). Opportunities for environmental crime: A test of situational crime prevention theory. *The British Journal of Criminology*, *53*(6), pp. 1178 – 1200. https://doi.org/10.1093/bjc/azt036

IBM Corp. (2016). *IBM SPSS Statistics for Windows, Version 24.0*. IBM Corp.

Kempa, M. (2010). Combating white-collar crime in Canada: Serving victim needs and market integrity. *Journal of Financial Crime*, *17*(2), 251–264.

Kemp, T. (2015). *The power and problem of privilege in cybersecurity*. Forbes (June 1, 2015). Retrieved from
https://www.forbes.com/sites/frontline/2015/06/01/the-power-and-problem-of-privilege-in-cybersecurity/?sh=7074f1f30502

Kim, J., Park, E. H., & Baskerville, R. L. (2016). A model of emotion and computer abuse. *Information & Management*, *53*(1), 91-108. doi:10.1016/j.im.2015.09.003

Królewiak, K. (2017). Need for Power. In: Zeigler-Hill, V., Shackelford, T. (eds) Encyclopedia of Personality and Individual Differences. Springer, Cham. https://doi.org/10.1007/978-3-319-28099-8_539-1

Legg, J. (June 10, 2022). It's time for the C-suite to protect themselves against cyberattacks. Forbes (June 10, 2022). Retrieved from https://www.forbes.com/sites/forbesbusinesscouncil/2022/06/10/its-time-for-the-c-suite-to-protect-themselves-against-cyberattacks/?sh=3dd1ed695684

Lowry, P. B., Posey, C., Bennett, R. B. J., & Roberts, T. L. (2015). Leveraging fairness and reactance theories to deter reactive computer abuse following enhanced organisational information security policies: an empirical study of the influence of counterfactual reasoning and organisational trust. *Information Systems Journal, 25*(3), 193-273. doi:10.1111/isj.12063

MacKinnon, D., Fairchild, A.J., & Fritz, M.S. (2007). Mediation Analysis. *Annual Review of Psychology*, *58*, pp. 593 – 614.

McClelland, D.C. & Burnham, D.H. (2003). *Power is the great motivator*. Harvard Business Review (January 2003). Retrieved from https://hbr.org/2003/01/power-is-the-great-motivator

McClelland, D. C. (1965). Toward a theory of motive acquisition. *American Psychologist, 20*(5), 321–333. https://doi.org/10.1037/h0022225

Molho, C., Balliet, D., & Wu, J. (2019). Hierarchy, power, and strategies to promote cooperation in social dilemmas. *Games, 10*(1), 1–12.

Moon, B., Lee, N., & Bourdage, J.S. (2021). Personalized and socialized need for power: Distinct relations to employee traits and behaviors. *Canadian Journal of Behavioural Science*, *54*(1), 28 – 39.

O'Boyle, E. H., Forsyth, D. R., & O'Boyle, A. S. (2011). Bad apples or bad barrels: An examination of group- and organizational-level effects in the study of counterproductive work behavior. *Group & Organization Management, 36*(1), 39–69. https://journals.sagepub.com/doi/10.1177/1059601110390998

Ponemon Institute LLC. (2022). *Cost of insider threats: Global report*. Ponemon Institute LLC.

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

Williams, M. L., Levi, M., Burnap, P., & Gundur, R. V. (2019). Under the corporate radar: Examining insider business cybercrime victimization through an application of routine activities theory. *Deviant Behavior, 40*(9), 1119–1131.

Willison, R., & Backhouse, J. (2006). Opportunities for computer crime: considering systems risk from a criminological perspective. *European Journal of Information Systems, 15*(4), 403-414. doi:10.1057/palgrave.ejis.3000592

Willison, R., & Warkentin, M. (2013). Beyond deterrence: An expanded view of employee computer abuse. *MIS Quarterly*, *37*(1), 1-20.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: insights from justice, deterrence and neutralization perspectives. *Information Systems Journal*, *28*(2), 266-293. doi:https://doi.org/10.1111/isj.12129

Xu, F., Luo, X., & Hsu, C. (2020). Anger or fear? Effects of discrete emotions on employee's computer-related deviant behavior. *Information & Management, 57*(3), 103180. doi:https://doi.org/10.1016/j.im.2019.103180

VentureBeat (February 15, 2022). Report: Only 21% of enterprises use zero trust architecture. Retrieved from https://venturebeat.com/security/report-only-21-of-enterprises-have-adopted-zero-trust-architecture/