A Computational Social Science Approach to Examine the Duality between Productivity and Cybersecurity Policy Compliance within Organizations

Clay Posey[1] and Matthew Canham[2]

1 College of Business, University of Central Florida, Orlando, FL 32826 USA
2 Institute for Simulation and Training, University of Central Florida, Orlando, FL 32826 USA
Clay.Posey@ucf.edu

Abstract. Organizational employees often face conflicting responsibilities in their daily tasks. On one hand, employees must be productive members of their organization; on the other, they must perform their tasks while conforming to cybersecurity policies thereby causing a reduction in their performance rates. Such compliance can also lead to increases in stress, which might already be relatively high given the workload placed on the employees.

In addition to this dichotomy, organizations vary significantly in the amount of emphasis placed on their productivity and cybersecurity goals. Employees use this and other information when making determinations about whether to follow cybersecurity policies for a given task. And while some of these determinations are based in rational cost-vs-benefits analyses, many are born out of habituation.

Despite the importance of understanding individual-level decision making in regard to performance—both in productivity and compliance—little research has examined how such micro-level actions aggregate to macro-level phenomena within organizations. Given this opportunity, we explore how varying workload, productivity and compliance emphases (i.e., culture), and the degree by which compliance decreases productivity (i.e., friction) for a given task affects a simulated organization's employees' stress levels. Moreover, we investigate how these factors (including rationality vs habituation, morality) combine to form emergent noncompliance patterns at the organizational level.

Keywords: Cybersecurity compliance, Workforce modeling, Productivity modeling, Decision making, Habituation.

1 Introduction

Organizational supervisors aim to guide their subordinates in ways that improve the performance of their individual units. One mechanism used to help meet these goals is the implementation of information technologies (IT) that create, acquire, store, manipulate, and/or disseminate significant amounts of operational data. Despite IT's benefits, organizations must deploy cybersecurity policies to protect informational assets from

their threats; and insiders must adapt their work procedures to these heightened controls. Consequently, insiders often believe they must decide between performing some of their tasks in a completely secure fashion and completing all their tasks in a somewhat secure fashion. This perceived imbalance between security and productivity often leads to insider circumvention of policies and procedures [1]—a widespread phenomenon termed *non-malicious noncompliance*. True, high-profile malicious insider threat cases such as Chelsea (Bradley) Manning, Edward Snowden, and Reality Winner illustrate the damage that can be inflicted by insider-led security breaches; however, the bulk of an organization's attack surface lies within unintentional insider threats—non-malicious insiders acting outside established security policies and procedures [2].

We aim to investigate how these individual-level production and compliance trade-off decisions affect entire organizations, thereby extending research in insiders' cybersecurity compliance that is very much limited to individual-level knowledge. Through embedding foundations from cognitive science, psychology, and organizational behavior in digital agents, we explore how perceived culture for productivity and cybersecurity policy compliance, levels of rationality and morality, work load, and friction (i.e., the amount of energy exerted by an agent to do a unit of work in a compliant manner) affect a simulated organization's productivity and compliance at the macro level.

1.1 Relationship to Extant Research

Previous cybersecurity policy compliance research shows that a variety of factors influence an individual's compliance intentions. These factors include attitude toward the policies [3], social factors like normative beliefs and subjective norm [4, 5], and self-efficacy beliefs [3, 5]. Further, insiders' motivations to protect information resources are also influenced by perceived response costs and efficacies [6], and self-report habituation has also been linked to compliance [4].

As stated previously and notwithstanding their benefits, these efforts are limited to individual-level compliance only and fail to show how, and when, micro-level compliance activities influence aggregate structures. Such research requires a computational approach. A few efforts have examined compliance and other cyber-relevant activities from a computational social science and/or complex adaptive systems perspective [7-9], though there is much left to explore. We now describe the foundations with which we endow our simulation.

Rationality vs. Habituation: The Dual-Process Theory of Decision Making.

The Dual-Process Theory of decision making states that humans rely upon two "systems" for making decisions; a deliberative, 'rational' system and an automatic system. [10-13]. The automatic system is very fast, involuntary, and inaccessible by conscious introspection. Subjectively, the automatic system feels intuitive and effortless, however it can also be highly error prone. Automatic processing can be either learned or inherited through biological processes [13]. Conversely, the relatively slower and

consciously directed deliberative system is a process that subjectively feels rational and effortful. Neuroscience research has detailed the distinctiveness of these systems and that habit reliance is an automatic process activated by environmental cues [14]. More recent studies within this literature suggests that stress leads to cortical processing shifts from the prefrontal cortex and hippocampus to the amygdala and dorsal striata at the cost of prefrontal (i.e., deliberative) processing [15]. Similarly, human factors research shows that individuals become more reliant upon automatic processing when fatigued or stressed [16]. Accordingly, insiders may increasingly rely on habituation rather than deliberative decision making when under high cognitive load and/or emotional duress.

Role Overload, Stress, and Work Strain.

Industrial-organizational psychologists and organizational behaviorists have identified how employees' overload and stress perceptions lead to negative workplace outcomes like low levels of job satisfaction and organizational commitment [17] and high levels of incivility and aggression [18]. Employee frustration also results in resistance to manager demands [19]. Moreover, job stressors that hinder the performance of normal organizational tasks give rise to anger, which in turn lead to decreased performance and counterproductive behaviors [20, 21].

Morality.

Despite an outcome of an employee's rational, deliberative costs-vs-benefits analysis that would result in noncompliance, the individual's morality or trait-based moral character likely prohibits such action through behavioral regulation. Morality, certain moral reasoning stages, and self-control have been shown to relate significantly to important organizational behaviors including counterproductive workplace and organizational citizenship behaviors [22] and even cybersecurity policy compliance [23, 24].

2 Design

We used the NetLogo 6.0.2 modeling software platform [25]. Due to space constraints, we detail our experimental design, based on the ODD protocol [26], in Table 1.

Table 1. Experimental Design

Purpose	To explore the duality between insiders' productivity and cybersecurity compliance
Entities, state variables, and scales	Entities: 25 agents Variables and scales: **Friction** (i.e., max amount of effort due to policy compliance for a given task): Scale (0.2 - 1.0, 0.2 increments); **Average workload**: Scale (70-100, 5 increments); **Culture** (i.e., the ratio for reward for productivity relative to the reward for compliance): Scale (5, 3.5, 2, 1, 1/2, 1/3.5, 1/5); **Morality**: Scale (0.75-0.95, 0.10 increments); **Rationality threshold** (i.e., average threshold when an agent will rely on habituation vs. rational-choice decision making): Scale (0.80, 0.90) Simulation scales: 100 ticks equal one work day in the organization

Basic process overview	Process overview: (1) Endow agents with features taken from GUI (2) Load agents' daily work queues (3) If work available, do work, else reduce stress (4) Select do-rationality or do-habituation (5) In do-rationality, compare **Culture** against perceived compliance **Friction**; if rewards > costs, do-work-with-security else do-work-wo-security if random die roll above **Morality** (6) Decrement work queue by one productivity rate if do-work-wo-security vs. (productivity rate * (1 - **Friction**)) if do-work-with-security (7) Stress increases by small amount when work is completed but decreases at the beginning of each day if work in queue <= productivity capability
Basic principles	Agents must accomplish work but also decide whether to follow cybersecurity policy, which slows productivity; High workloads produce stress on agents; Stress influences agents' decision-making paths; In rational choice decisions, agents try to balance rewards vs costs, and morality regulates decisions to engage in noncompliance
Emergence	Patterns of overall stress levels, cybersecurity policy noncompliance, and productivity
Adaptation	Agents exhibit some adaptation in decision choice due to perceived stress levels
Objectives	To reduce stress but match the organization's culture for productivity and security
Learning	Agents rely on a previous two-weeks' worth of actions when engaging in habituation; habit is assumed to form, on average, in a two-week period
Sensing	Agents can sense when a day's workload is beyond their productivity capacity
Stochasticity	Agent selection is randomized through every tick of experiment
Observation	Data were assessed at the end of the experiments. Means of overall stress, noncompliance, compliance, work-queue size, and amount of work units delayed were analyzed. 35 simulations per unique scenario were ran (more than 50,000 total runs)
Initialization	Agents endowed with data taken randomly from normal distributions with the GUI inputs as means
Sub-models	reduce-stress, do-work, do-rationality, do-habituation, do-work-with-security, do-work-wo-security

3 Key Results

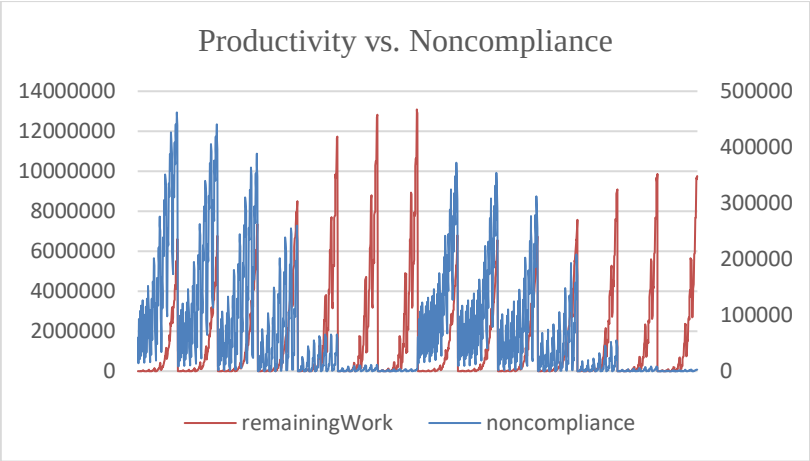
Several findings emerged from our analysis. Those that were expected include:

- As culture focuses on productivity over security, noncompliance increases
- As culture focuses on security over productivity, average work-queue sizes and delayed work units increase
- As workload increases, noncompliance increases
- As friction increases, noncompliance, average work-queue sizes, and delayed work units increase
- As morality increases, noncompliance decreases

More emergent findings include:

- As habituation increases, delayed work units in the organization decreases
- Some level of noncompliance exists in all conditions
- Average stress levels are driven more by workload than culture
- As productivity increases, noncompliance increases
- Once culture focuses on security over productivity, noncompliance decreases dramatically

Fig. 1. Productivity versus Non-Compliance



4 Conclusion

The need for organizations to operate efficiently and effectively is being pitted against the requirement to protect information assets. Employees are now pressured to perform at high levels while following cybersecurity policies with exactness. This research assists in understanding how the forces on insiders and their subsequent actions affect entire organizations. As such, this research can inform managers on the effective design and of job tasks and cybersecurity policies in production-oriented environments.

References

1. Posey, C., Roberts, T.L., Lowry, P.B., Hightower, R.T.: Bridging the divide: A qualitative comparison of information security thought patterns between information security professionals and ordinary organizational insiders. Information & Management 51, 551-567 (2014)
2. Greitzer, F.L., Strozer, J.R., Cohen, S., Moore, A.P., Mundie, D., Cowley, J.: Analysis of unintentional insider threats deriving from social engineering exploits. In: 2014 IEEE Security and Privacy Workshops, pp. 236-250. IEEE, (Year)
3. Bulgurcu, B., Cavusoglu, H., Benbasat, I.: Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly 34, 523-548 (2010)
4. Moody, G.D., Siponen, M., Pahnila, S.: Toward a unified model of information security policy compliance. MIS Quarterly 42, (2018)
5. Herath, T., Rao, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations. European Journal of Information Systems 18, 106-125 (2009)
6. Posey, C., Roberts, T.L., Lowry, P.B.: The impact of organizational commitment on insiders' motivation to protect organizational information assets. Journal of Management Information Systems 32, 179-214 (2015)

7. Burns, A., Posey, C., Courtney, J.F., Roberts, T.L., Nanayakkara, P.: Organizational information security as a complex adaptive system: insights from three agent-based models. Information Systems Frontiers 19, 509-524 (2017)
8. Carley, K.M., Morgan, G.P.: Inadvertent leaks: exploration via agent-based dynamic network simulation. Computational and Mathematical Organization Theory 22, 288-317 (2016)
9. Sokolowski, J.A., Banks, C.M., Dover, T.J.: An agent-based approach to modeling insider threat. Computational and Mathematical Organization Theory 22, 273-287 (2016)
10.Croskerry, P., Singhal, G., Mamede, S.: Cognitive debiasing 1: origins of bias and theory of debiasing. BMJ Quality & Safety 22, 58-64 (2013)
11.Kahneman, D.: Thinking, fast and slow. Farrar, Strauss, and Giroux, New York, NY (2011)
12.Morewedge, C.K., Kahneman, D.: Associative processes in intuitive judgment. Trends in Cognitive Sciences 14, 435-440 (2010)
13.Stanovich, K.E., West, R.F.: Individual differences in reasoning: Implications for the rationality debate? Behavioral and Brain Sciences 23, 645-665 (2000)
14.Neal, D.T., Wood, W., Wu, M., Kurlander, D.: The pull of the past: When do habits persist despite conflict with motives? Personality and Social Psychology Bulletin 37, 1428-1437 (2011)
15.Wirz, L., Bogdanov, M., Schwabe, L.: Habits under stress: mechanistic insights across different types of learning. Current Opinion in Behavioral Sciences 20, 9-16 (2018)
16.Tay, S.W., Ryan, P., Ryan, C.A.: Systems 1 and 2 thinking processes and cognitive reflection testing in medical students. Canadian Medical Education Journal 7, 97-103 (2016)
17.Jones, E., Chonko, L., Rangarajan, D., Roberts, J.: The role of overload on job attitudes, turnover intentions, and salesperson performance. Journal of Business Research 60, 663-671 (2007)
18.Taylor, S.G., Kluemper, D.H.: Linking perceptions of role stress and incivility to workplace aggression: The moderating role of personality. Journal of Occupational Health Psychology 17, 316-329 (2012)
19.Lawrence, T.B., Robinson, S.L.: Ain't misbehavin: Workplace deviance as organizational resistance. Journal of Management 33, 378-394 (2007)
20.Rodell, J.B., Judge, T.A.: Can “good” stressors spark “bad” behaviors? The mediating role of emotions in links of challenge and hindrance stressors with citizenship and counterproductive behaviors. Journal of Applied Psychology 94, 1438-1451 (2009)
21.Tarafdar, M., Tu, Q., Ragu-Nathan, T.: Impact of technostress on end-user satisfaction and performance. Journal of Management Information Systems 27, 303-334 (2010)
22.Cohen, T.R., Panter, A.T., Turan, N., Morse, L., Kim, Y.: Moral character in the workplace. Journal of Personality and Social Psychology 107, 943 (2014)
23.Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., Vance, A.: What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems 18, 126-139 (2009)
24.Hu, Q., West, R., Smarandescu, L.: The role of self-control in information security violations: Insights from a cognitive neuroscience perspective. Journal of Management Information Systems 31, 6-48 (2015)
25.Wilensky, U.: NetLogo. http://ccl.northwestern.edu/netlogo/. Center for Connected Learning and Computer-Based Modeling. Northwestern University, Evanston, IL (1999)
26.Grimm, V., Berger, U., DeAngelis, D.L., Polhill, J.G., Giske, J., Railsback, S.F.: The ODD protocol: a review and first update. Ecological modelling 221, 2760-2768 (2010)