Barking Up the Wrong Tree? Reconsidering Policy Compliance as a Dependent Variable within Behavioral Cybersecurity Research

W. Alec Cram
University of Waterloo
wacram@uwaterloo.ca

John D'Arcy
University of Delaware
jdarcy@udel.edu

Abstract

A rich body of research examines the cybersecurity behavior of employees, with a particular focus on explaining the reasons why employees comply with (or violate) organizational cybersecurity policies. However, we posit that this emphasis on policy compliance is susceptible to several notable limitations that could lead to inaccurate research conclusions. In this commentary, we examine the limitations of using cybersecurity policy compliance as a dependent variable by presenting three assertions: (1) the link between policy compliance and organizational-level outcomes is ambiguous; (2) policies vary widely in terms of their clarity and completeness; and (3) employees have an inconsistent familiarity with their own organization's cybersecurity policies. Taken together, we suggest that studying compliance with cybersecurity policies reveals only a partial picture of employee behavior. In response, we offer recommendations for future research.

Keywords: Cybersecurity, information security, policy, compliance, violation, employee behavior.

1. Introduction

Organizational policies have long played a central role in behavioral cybersecurity research (Cram et al., 2017; Moody et al., 2018). Indeed, past research points to employee compliance[1] with cybersecurity policies[2] as an important tool to reduce risky employee behaviors that can lead to negative downstream consequences such as data breaches and network intrusions (Balozian & Leidner, 2017; Ormond et al., 2019; Yazdanmehr & Wang, 2021). Although there is little dispute that accidental, inadvertent, and malicious employee behavior can contribute to cybersecurity incidents (IBM Security, 2021; Verizon, 2021), we assert that there are certain limitations that stem from relying on measures of policy compliance as a proxy for an employee's overall cybersecurity behavior. Specifically, we argue that the current focus on cybersecurity policy compliance as a dependent variable has the potential to lead to inaccurate research conclusions.

Behavioral cybersecurity research has reached a high level of maturity in recent years, as evidenced by recent literature reviews that encompass over 100 publications, including Balozian and Leidner (2017) and Cram et al. (2019). This body of research has relied heavily on employee compliance with cybersecurity policies as its most common dependent variable (refer to Table 1 for a sample of prominent papers published over the past five years). This research focus allows insights to be gleaned in regard to the individual-level characteristics (e.g., personal ethics, attitude, self-efficacy) that are associated with policy-compliant behavior, as well as the potential links between managerial actions (e.g., management support, rewards, training) and compliance. Although we do not dispute the valuable contribution that this research has made or the significant cumulative tradition it has established, we submit that the line of inquiry has laid bare some opportunities for reflection and potential improvements in the future.

Recently, scholars have begun to evaluate the various approaches used to study policy compliance. This includes highlighting the relative benefits of examining actual policy compliance compared to intended policy compliance (Jenkins et al., 2021; Vance et al., 2014), as well as the differences between compliance with specific versus general policies (Aurigemma & Mattson, 2019; Cram et al., 2019; Siponen & Vance, 2014); however, our view is that it is the study of policy compliance in any form that is

[1] In keeping with past literature, such as Cram et al. (2019), we use the term "cybersecurity policy compliance" to refer to compliance research, as well as studies considering violation, non-compliance, misuse, and abuse.

[2] Consistent with past views (e.g., Baskerville & Siponen, 2002; Whitman, 2008), we recognize the existence of three broad types of cybersecurity policies: enterprise policies (i.e., a strategic direction for cybersecurity), technical policies (i.e., security maintenance and configuration), and issue-specific policies (i.e., guidelines for employee behavior related to organizational technology resources). Our focus in this paper is on issue-specific policies.

URI: https://hdl.handle.net/10125/103137
978-0-9981331-6-4

subject to a number of fundamental limitations. In particular, we point out three specific shortcomings associated with the study of policy compliance as a dependent variable. First, we suggest that the links between policy compliance and tangible, organizational-level outcomes (e.g., data breaches) are ambiguous, at best. Even though we acknowledge that, generally speaking, increased policy compliance and decreased policy violation is "good", we also suggest that researchers cannot definitively conclude that compliance will reduce the frequency or severity of cybersecurity incidents. Second, we argue that the quality of cybersecurity policies varies widely across organizations in terms of their clarity and completeness. Therefore, where groups of employees have divergent perceptions of what exactly compliant behavior entails, research results may draw unreliable conclusions. Finally, we contend that employees often have an inconsistent knowledge of their own organization's cybersecurity policies (regardless of their quality), which potentially makes their own compliance assertions unpredictable.

Taken together, we suggest that these three shortcomings could lead researchers to draw inaccurate conclusions. For example (pertaining to the "inconsistent knowledge" shortcoming pointed out just above), a typical behavioral cybersecurity study collects data from several hundred survey participants and asks questions to solicit responses such as "I intend to comply with the requirements of my organization's cybersecurity policy". Although researchers implicitly assume that participants have a full understanding of their organizations' policies, practitioner reports suggest that this is true for only about 12% of employees (Kaspersky Lab, 2018). Consequently, in cases where a sizable portion of survey participants have not recently read their organization's policy or do not fully understand the policy contents, the resulting data may be indicative of a participant's (potentially inaccurate) perception of the cybersecurity policy, rather than their company's actual policy. As a result, employees may inadvertently overestimate their compliance intentions due to their flawed understanding of the policy requirements (e.g., new requirements could have been added to the policy since the participant last read it) or underestimate their compliance intentions (e.g., a participant has only ever skimmed the company policy, but assumes it is difficult to follow). The ensuing theoretical insights could therefore overlook significant relationships or reveal erroneous relationships.

Despite this perspective, we do not call for researchers in the field to abandon their study of cybersecurity policy compliance behavior; however, we suggest that compliance behavior as an outcome variable might be better suited for specific situations, such as when participants all belong to a single organization with a single cybersecurity policy or where researchers can control for policy-specific variability. Outside of those situations, we propose several alternative paths for researchers to consider and offer some actionable recommendations for future research.

2. Conceptual background

Early studies in the behavioral aspects of cybersecurity, beginning with Straub (1990) and Straub and Nance (1990), focused on employee actions referred to as "computer abuse" and considered the resulting cybersecurity incidents and the associated financial losses experienced by organizations. It was not until later work, such as Harrington (1996), when researchers began to move away from the actual organizational-level consequences and oriented their focus towards adherence to organizational policies. Since that time, the majority[3] of research associated with cybersecurity policies has focused on employee compliance as a dependent variable.

Past reviews, such as Balozian and Leidner (2017) and Cram et al. (2019), have thoroughly synthesized this literature, which has primarily sought to uncover the various antecedents to compliant or non-compliant behavior. These antecedents are consequently viewed as opportunities for managers to improve organizational security (e.g., hire employees with stronger ethics). However, the connection between compliance with cybersecurity policies and actual downstream consequences such as data breaches, has been strongly inferred, but not robustly validated. In the few studies that do consider the connection, results are mixed, with some studies supporting the relationship, while others find no significant link (e.g., Doherty & Fulford, 2005; Wiant, 2005). However, researchers have called for more work in this area. For example, Cram et al. (2017) specifically note, "There is a paucity of empirical studies that clearly establish that compliance directly results in desirable organizational objectives. Although this relationship is widely assumed to exist, few studies investigate the tangible benefits that can result" (p. 618).

A range of theoretical bases have been employed in the existing cybersecurity policy compliance research, including the frequent use of theory of planned

[3] In a comprehensive review of the cybersecurity literature, Cram et al. (2017) identified 114 publications associated with organizational cybersecurity policies. Of these, 81 papers examined the organizational and individual factors associated with policy compliance.

behavior, deterrence theory, and protection motivation theory (Moody et al., 2018). Although each of these theories employ different main constructs, behavioral intention is the primary predictor in each case. Recently, scholars have begun to highlight certain limitations regarding the field's approach to studying policy compliance, including the focusing on an individual's behavioral intention to comply rather than on their actual compliance behavior (Jenkins et al., 2021; Vance et al., 2014), as well as the difference between measuring an employee's intention to comply with a formal policy versus a broader, more discretionary intention to protect information assets (Burns et al., 2018; Hsu et al., 2015). Literature has also pointed out the differences between focusing on employee compliance with a general cybersecurity policy versus a specific policy (Aurigemma & Mattson, 2019; Siponen & Vance, 2014). However, despite the concerns, policy compliance remains a core dependent variable in recent research.

Table 1. Recent Cybersecurity Policy Compliance Publications

Publication	Intention to Comply with Policy	Intention to Violate Policy
Barlow et al. (2018)	-	X
Farshadkhah et al. (2021)	-	X
Feng et al. (2019)	X	-
Goel et al. (2021)	X	-
Gwebu et al. (2020)	-	X
Herath et al. (2018)	-	X
Hina et al. (2019)	X	-
Jaeger et al. (2021)	X	-
Jenkins et al. (2021)	X	-
Jeon et al. (2020)	X	-
Ormond et al. (2019)	X	-
Rajab & Eydgahi (2019)	X	-
Sarkar et al. (2020)	-	X
Sharma & Warkentin (2019)	X	-
Silic & Lowry (2020)	X	-
Trang & Nastjuk (2021)	-	X
Yazdanmehr et al. (2020)	X	-
Yazdanmehr & Wang (2021)	X	-
Yoo et al. (2018)	X	-

The aim of this research is to consider the potential concerns surrounding the use of the cybersecurity policy compliance construct and, where alternatives exist, offer a proposed path forward.

2.1. Concerns with the cybersecurity policy compliance construct

Based on the approaches adopted in past research, as well as recent practitioner accounts, we note three primary concerns with the use of cybersecurity policy compliance as a dependent variable. We detail these concerns below, in the form of conjectures.[4]

2.1.1. Ambiguous links exist between policy compliance and organizational outcomes. Fundamentally, researchers examine policy compliance (both actual and intended) as an indicator of the extent that employee behavior will lead to consequential organization-level outcomes, such as data breaches or intrusions. Such behavior-incident links are well established and commonly referred to in behavioral cybersecurity publications (e.g., Balozian & Leidner, 2017; Bulgurcu et al., 2010; Herath & Rao, 2009). However, nearly all research stops at the measurement of policy compliance and does not formally connect employee behavior to downstream outcomes (i.e., policy violations lead directly to data breaches). For the few papers that do extend their analysis to the consequences of having cybersecurity policies in place, the findings are underwhelming. For example, Doherty and Fulford (2005) surveyed 219 IT managers in the United Kingdom and found no statistically significant relationship between the adoption of cybersecurity policies and the incidence or severity of breaches.[5]

Inferences are commonly drawn by researchers between policy non-compliance and security incidents by pointing to a recent security incident and an associated employee behavior (e.g., the data breach was enabled by an employee who disclosed their password during a phishing attack). However, this assertion is grounded in the risky employee behavior (the password disclosure) and not whether there happened to be a password policy in place that was violated.

Other work (e.g., Burns et al., 2018; Hsu et al., 2015) has highlighted the distinction between in-role expectations (i.e., a user's compliance with the policy-specified guidelines) and the extra-role behaviors (i.e., a user's broader, discretionary behaviors that go beyond

[4] We follow the approach adopted by Grover et al. (2020), who utilize conjectures as "theory-free suppositions formed on the basis of the currently incomplete information…and its potential impact. Our conjectures represent a 'prescientific' understanding along with related explanations and predictions…essentially presenting our best assessment of the likely consequences…given our understanding of how research knowledge is currently produced in our field" (p. 271).

[5] We acknowledge that both the rate of policy adoption and breach incidence/severity were provided by the same source (IT Managers) in this study. This relationship might be better tested with an objective measurement of data breaches, given that IT managers would seemingly have incentive to not report data breach incidents.

the formal policy guidelines). That is, employee compliance with policies is neither a necessary nor a sufficient condition to reduce the frequency or severity of organizational cybersecurity incidents. For example, employees may always comply with the organizational cybersecurity policy, but when a new attack vector emerges (e.g., a new vulnerability is discovered in the approved cloud storage system software) that the policy does not address, it is possible that an incident occurs through no fault of the employee. Likewise, employees may regularly violate policies (e.g., frequent use of prohibited cloud storage software), but no organizational-level incidents result. Although the study of employee compliance with cybersecurity policies provides important clues to the risk factors that can lead to organization-level issues, it is insufficient by itself to draw definitive conclusions pertaining to how protected or vulnerable an organization is to attack. This blind spot may help explain the common refrain in behavioral cybersecurity research papers that recognize the rising frequency of cybersecurity incidents, despite our ever-improving understanding of what leads employees to comply with policies. That is, we know the factors that lead employees to comply/violate organizational policies, but the factors that lead to cybersecurity incidents are—at least partly—different.

As an illustrative example, consider that Brad's company includes a policy that requires employees to only use the approved cloud-based data storage service for company data. Although Brad always adheres to the policy, a software vulnerability is discovered by hackers, who download and post all of his files to the internet. In comparison, consider that Lisa's company includes a policy that requires employees to only use the approved cloud-based data storage service for company data. Lisa dislikes the service's interface and violates the policy by using a non-approved service instead. Her service of choice did not contain a software vulnerability and her files remained safe. When considering the two scenarios from a research perspective, Brad complied with his company's policy, but ended up experiencing a data breach, whereas Lisa violated her company's policy, but did not experience a breach. As such, assuming that employee compliance with the cybersecurity policy will always correspond with reduced data breaches is inaccurate in these scenarios. As a result, we suggest:

> ***Conjecture 1:*** *Individual-level cybersecurity policy compliance is not a completely reliable predictor of organizational-level consequences (e.g., data breaches).*[6]

2.1.2. Variance in the clarity and completeness of cybersecurity policies. Cybersecurity policies within organizations are designed, implemented, and monitored to highly varying degrees (Doherty et al., 2009; Karlsson et al., 2017; Siponen & Vance, 2014). This variance includes core elements of policy quality, including static versus regularly updated policies; concise versus wordy policies; and clear language versus highly technical language. A recent practitioner-oriented commentary pointed to the importance of the issue, arguing that, "at its core, cybersecurity depends on communication. Outdated security policies that are poorly communicated are equally as dangerous as substandard software code and other flawed technical features" (Weber, 2022).

Although some modest research attention has been paid to the development of cybersecurity policies, the approaches tend to vary widely (Paananen et al., 2020). For example, some policies are created by beginning with a risk assessment (e.g., Flowerday & Tuyikeze, 2016), while others are not (e.g., Ward & Smith, 2002). Similarly, ongoing policy maintenance is highlighted as a key step by some authors (e.g., Howard, 2003), but not by others (e.g., Baskerville & Siponen, 2002).

Despite these variations in the cybersecurity policies that are in place within organizations, there is relatively little research that examines how the characteristics of a policy, such as its quality, relate to different levels of employee compliance. This is further confounded by few studies that draw participants from a single organization that utilizes a shared cybersecurity policy, in favor of collecting data from a range of participants employed at many different companies (and thus different policies). In one example, Stahl et al. (2012) undertook a critical evaluation of cybersecurity policies in 25 institutions across the UK healthcare sector. From a clarity perspective, the authors note that "having carefully reviewed the policies, it became clear that there was a significant amount of ambiguity, in particular with respect to the policies' objective and intended targets, as well as significant evidence of the use of jargon and unfamiliar language" (p. 85). Later, they go on to note that "…the comprehensibility of the policy documents was often obscured by the use of very technical language" (p. 86).

Most researchers discuss cybersecurity policies as either being complied with or violated by employees. In practice, this determination may depend on whose perspective compliance is evaluated from. That is, managers who design and implement cybersecurity policies may have a clear understanding of behavior that is compliant (or not). However, employees may

[6] We recognize that this conjecture suggests the absence of a relationship, rather than the existence of a relationship; however, we believe this to be relevant as it challenges the prevailing wisdom within the current policy compliance literature.

interpret the rules differently and comply/violate to varying extents (e.g., honest, inadvertent errors versus malicious actions versus emotion-driven [e.g., lazy, fatigued, stressed, etc.] actions). Policies that are both clear (i.e., they unambiguously outline employee expectations) and complete (i.e., they include all necessary information for the employee) can help to combat this challenge; unfortunately, cybersecurity policies are notorious for their technical jargon, unnecessary length, and ambiguous language (Goel & Chengalur-Smith, 2010; Stahl et al., 2012). In some cases, a well-intentioned employee may inadvertently violate the policy because they misunderstood an ambiguous directive. In other cases, employees may believe they are acting in compliance with a policy, but are actually non-compliant because they failed to read a technical detail that was buried in an online attachment. In research where either policy compliance intentions are measured (e.g., "I am likely to follow organizational security policies") or actual policy compliance is measured (e.g., "I follow organizational security policies"), participants need to make a judgement on what exactly a compliant/non-compliant behavior is, based on a perception of their organization's cybersecurity policy. Since each organization's policy is different and each participant's view of that policy is subject to interpretation, research that studies policy compliance based on employee self-reports may be susceptible to unreliable measurement (Siponen & Vance, 2014).

As an illustrative example, consider the scenario of DeShawn, who works at a company with a well-written, clear, and complete cybersecurity policy. He reports that his activities are always in compliant. In comparison, Sherry works in a company with a poorly written policy, including the extensive use of jargon, acronyms, and technical language. Although Sherry reports that her activities are always in compliance with the policy, she acknowledges that there is a degree of interpretation required in determining what behaviors are permitted and isn't sure that her manager would concur that she is always in compliance. When considering the two scenarios from a research perspective, both DeShawn and Sherry report that they are compliant with their company's policy, but Sherry's behavior is potentially more varied than DeShawn's, due to the poor quality of her organization's policy. That is, drawing conclusions that compare the behavior of DeShawn and Sherry may be inaccurate. As a result, we propose:

> ***Conjecture 2:*** *Individual-level cybersecurity policy compliance is not a completely reliable dependent variable due to variance in the clarity and completeness of cybersecurity policies across organizations.*

2.1.3. Inconsistencies in employee familiarity with cybersecurity policies. Both practitioner accounts and research results indicate that many employees are unaware and unfamiliar with the details of their own organization's cybersecurity policies. Although past research supports a link between an employee's awareness of technology/security issues and employee compliance (Bauer & Bernroider, 2017; Dinev et al., 2009), as well as a link between security training and employee compliance (Goo et al., 2014; Hwang et al., 2017), reports from practice suggest that a notable proportion of employees are not fully informed of their cybersecurity expectations. For example, Shahbaznezhad et al. (2020) found that 56% of respondents answered between 1 and 4 on a scale of 1 (*completely unaware*) to 7 (*completely aware*) regarding their level of awareness of the organizational policy on phishing, while only 24% answered that they were *completely aware*. This result is in keeping with Kaspersky Lab's (2018) finding that only 12% of employees have a full understanding of their organization's cybersecurity policies.

Since much of the current compliance-oriented research asks employees to report either their intended behavior relative to the cybersecurity policy (e.g., "I intend to comply with the requirements of the ISP of my organization in the future"; Bulgurcu et al, 2010, p. 536) or actual behavior relative to the cybersecurity policy (e.g., "How often do you violate the ISP rules of your organization?"; Feng et al., 2019, p. 1677), reliable data might only come from those employees who have knowledge of exactly what their organization's policies are (Siponen & Vance, 2014). In effect, participants who are not very familiar with the content of their organization's cybersecurity policy are actually reporting their compliance behavior based on their incomplete and/or potentially incorrect understanding of the cybersecurity policy, rather than a perception based on the actual, complete cybersecurity policy that is in place.

Further, as new policies are periodically added and/or updated (Paananen et al., 2020), they may be viewed as a "moving target" for busy employees who may find it difficult to remain fully aware of them. This includes a knowledge gap for employees about what practical behaviors they should (or should not) be undertaking. For example, in their review of UK healthcare policies, Stahl et al. (2012) found that "…significant aspects of the policies' implementation had been missed or suppressed from the discourse. In particular, the message that all employees are personally responsible for the security of the information and systems that they use comes across extremely strongly, but the policies tend to be remarkably quiet on advising staff on how they should discharge these

responsibilities" (p. 87). As well, since managers can be inconsistent in enforcing policies or levying penalties for non-compliance, many employees do not make it a point to be clear on exactly what the rules are (in comparison to, say, harassment policies or overtime policies that are more likely to lead to disciplinary penalties or financial benefits).

As an illustrative example, consider the situation of Anika, whose company requires her to review the content of the cybersecurity policy each year and formally agree that she is aware of her responsibilities. She does so and reports that her activities are always in compliance with the policy. In comparison, Owen's company made mention of the cybersecurity policy when he was hired five years ago. As far as he knows, the policy hasn't changed much and is available somewhere on the company intranet. He reports that his activities are always in compliance with the policy. When considering the two scenarios from a research perspective, both Anika and Owen report that they are compliant with their company's policy, but Owen's behavior is potentially more varied than Anika's because of his limited familiarity with the policy. That is, drawing conclusions that compare the behavior of Anika and Owen may be inaccurate. Therefore, from these ideas, we suggest:

> ***Conjecture 3:*** *Individual-level cybersecurity policy compliance is not a completely reliable dependent variable due to variance in employee familiarity with organizational cybersecurity policies.*

The three conjectures noted above represent conclusions based on anecdotal practitioner accounts, as well as inferences from research results. In the following section, we consider the methodological alternatives available to researchers studying behavioral cybersecurity phenomenon.

3. Discussion and Future Research Directions

Although our conjectures highlight three key concerns stemming from the use of compliance with cybersecurity policies as a dependent variable, we do not argue that cybersecurity policy compliance research should be abandoned or that the existing findings are invalid. Rather, we believe that one option is for future research to deploy the variable in circumstances where its limitations can be accounted for.

For example, researchers could continue studying cybersecurity policy compliance but focus data collection activities on single organizations. By doing so, researchers could independently evaluate the clarity and completeness of the policy that employees would be responding to during data collection. By reporting on the characteristics of the company's policy in the findings, it would alleviate the cross-company comparison concerns highlighted in Conjecture 2.

Another option for researchers studying compliance with cybersecurity policies is to control for employee familiarity with cybersecurity policies. For example, by including survey questions that probe when the participant last read the policy and how they would rate their understanding of the policy, researchers could at least partly account for inaccurate results that could stem from employees who are unfamiliar with the policies they are expected to comply with. This would address concerns associated with Conjecture 3.

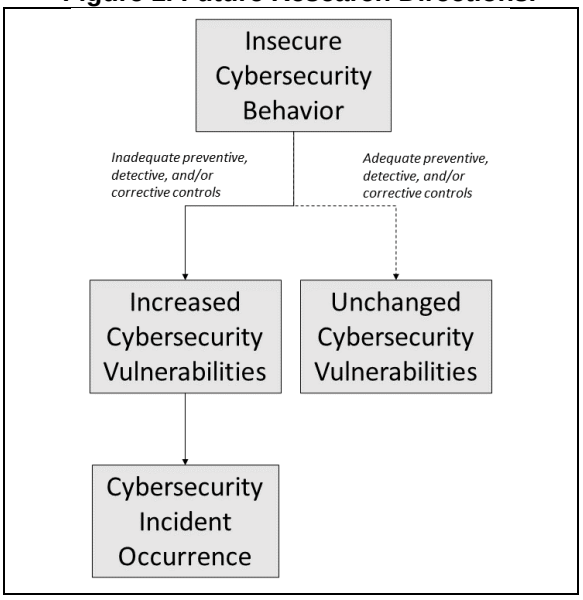
Alternatively, cybersecurity researchers could seek out other dependent variable options that are not solely oriented towards policy compliance. We propose that orienting studies around a more risk-based view of cybersecurity (Boehm et al., 2019), could allow researchers to focus on: (1) the *insecure behavior* of employees; (2) the *cybersecurity vulnerabilities* associated with insecure employee behavior; and (3) the *cybersecurity incidents* associated with insecure employee behavior. It is important to note that we consider these constructs from a temporal viewpoint, in that some insecure behaviors can lead to an increase in vulnerabilities, which can subsequently lead to an increase in incidents. Refer to Table 2 for a summary of the suggested dependent variable options.

The first non-policy-centric option is the study of insecure employee behavior. Here, researchers could measure actual or intended cybersecurity behavior (e.g., "I change my password every six months") rather than actual or intended behavior relative to a policy (e.g., "I comply with my organization's password policy"). We acknowledge that this approach has been adopted in a variety of past studies (e.g., Dinev et al., 2009; Jenkins & Durcikova, 2013; Jeske & van Schaik, 2017; Johnston & Warkentin, 2010). Apart from the concern that self-reported behavior doesn't always equate to actual behavior (e.g., due to a social desirability bias), a limitation of this approach is the acknowledgement that, although insecure behavior has the potential to cause harm to the organization, it does not lead to a definite increase in vulnerabilities or incidents in all cases. For example, best practices suggest that organizations design cybersecurity controls to be multi-layered and redundant (NIST, 2017). As such, risky behavior by an employee (e.g., not using anti-virus software on their personal computer) may be mitigated by other preventive or detective controls that limit or eliminate the incremental risk introduced by the employee (e.g., anti-virus tools are automatically run at the network level as well). Although we believe that the study of

insecure employee behavior has advantages relative to the study of policy compliance, it still has the potential to overstate the consequences for organizations (as noted in Conjecture 1), since the existence of mitigating controls (and thus the actual consequences of the insecure behavior) is not directly considered.

The second option addresses this shortcoming by examining the link between insecure employee behavior and an increase in cybersecurity vulnerabilities faced by the organization. Essentially, researchers could identify situations where insecure employee behavior is not being adequately prevented, detected, and/or corrected by existing organizational controls, thereby resulting in an increased possibility that a cybersecurity incident could occur. Auditors refer to the concept of *inherent risk*, which represents the possibility of an adverse event occurring if no controls were in place, while *residual risk* represents the possibility of an adverse event occurring, even with controls in place (Coetzee & Lubbe, 2014). The motivation for adopting a focus on the residual risk is to orient research efforts towards the employee behavior that has the potential to actually cause damage to the organization (i.e., where insufficient controls are in place), rather than focusing on behavior that is already being adequately mitigated. Siponen & Vance (2014) advocate for work in this area by encouraging the study of violations that are important and impactful to practice. Refer to Figure 1 for an illustration of this approach.

Figure 1. Future Research Directions.



For example, many organizations have instituted "bring your own device" (BYOD) guidelines for employees who wish to undertake company business using their personal technology devices. In the absence of administrative controls (e.g., communication to employees on what devices are permitted to be used) and technical controls (e.g., restricting user access to certain categories of company data), the risk that an insecure employee behavior (e.g., accidentally leaving a phone on the subway) could compromise a company's confidentiality is likely to be high. However, in the situation where a company implements a robust set of BYOD controls, such as restricting access to sensitive information, encrypting device data, and enabling remote-wipe capabilities, the risks of an incident are significantly diminished, even when insecure behaviors occur. In such a case (depicted on the right side of Figure 1), a researcher studying the extent that employees behave insecurely in their BYOD activities will result in less relevant findings (since the behavior is unlikely to result in any downstream consequences) compared to a researcher who studies the same behavior at a company who has poor BYOD controls. In short, this approach could help researchers focus their efforts on understanding insecure employee behavior that could actually result in damage, while disregarding behavior where damage is less likely.

To undertake a study oriented towards the links between employee behavior and cybersecurity vulnerabilities, researchers could focus on emerging high-risk cybersecurity threats where controls do not yet fully address the risks. Currently, the threat of ransomware and phishing is pronounced and many organizations struggle with a continued threat of attack and inadequate countermeasures (IBM Security, 2021). Alternatively, researchers could seek out firms where control weaknesses have already been identified, perhaps through audit findings or risk assessments.

Researchers pursuing this approach could focus on a single risky behavior (e.g., clicking on phishing emails) that has a high practical relevance to organizations. By going beyond generic explanations of employee behavior (e.g., employees will behave more securely when they expect to get sanctioned for insecure behavior) and instead focusing on specific, high-risk employee behaviors (e.g., the effectiveness of sanctions in avoiding ransomware attacks), researchers may be able to uncover novel theoretical applications, as well as more tailored, timely guidance for practitioners. For instance, such work could draw on neutralization theory (e.g., Barlow et al., 2013; Siponen & Vance, 2010), which suggests that individuals may rationalize their insecure behavior by concluding that it won't do any real harm. In cases where downstream controls are in place that will limit the impact of their actions, rationalizing employees may well be correct; however, research focused on insecure behaviors that lead to increased vulnerabilities could consider if employees will undertake rationalizations in the same way when they know their behavior is likely to result in harm. Such

research could take the form of a laboratory experiment that compares the propensity for employees to click on links in a phishing email in a scenario where they know their employer utilizes anti-ransomware tools versus a situation where no anti-ransomware tools are used.

A third direction for future research represents an extension of the previous option by examining the occurrence of specific organizational cybersecurity incidents that can actually be traced back to an insecure employee behavior. Anecdotal accounts commonly point to employees as being the "weak link" in the organizational cybersecurity ecosystem, but there is little empirical work that examines the extent to which employee behavior is considered a root cause of a cybersecurity incident.

To undertake research in this area, researchers could conduct case studies with organizations that have experienced cybersecurity incidents. Such research may provide an opportunity to apply qualitative methods that seek to generate rich, retrospective accounts of the root causes of a cybersecurity incident that has already occurred. Alternatively, researchers could undertake forward-looking inquiries that seek to collect longitudinal data leading up to a future cybersecurity incident. For example, a field study could investigate if the effectiveness of cybersecurity warnings (or "fear appeals") disseminated by IT departments diminish over time. Researchers could collect data at a single company (say, monthly over the course of a year) on the frequency of cybersecurity warnings, insecure employee behavior, and the identification of actual cybersecurity incidents. Results could help shed light on how employees respond to warnings over time and if this changing behavior corresponds with an increased frequency of actual cybersecurity incidents.

Table 2. Cybersecurity Policy Compliance DV Improvements

Dep. variable	Considerations/Areas of Focus
Compliance/ non-compliance with cyber-security policy	Focus on single organizations, where policy clarity/completeness can be independently evaluated.
	Control for cybersecurity policy familiarity by employees.
Insecure cybersecurity behavior	Focus on risky employee behavior, rather than on whether the behavior is a compliant or non-compliant act relative to a policy.
Cybersecurity vulnerabilities	Focus on the link between an employee's insecure behavior and an increase in organizational cybersecurity vulnerabilities.
Cybersecurity incident occurrence	Focus on the link between a cybersecurity vulnerability originating from an employee's insecure behavior and an actual cybersecurity incident.

We also acknowledge that empirical validation of our conjectures would further make the case for the alternatives noted above. For Conjecture 1 (policy compliance is an unreliable predictor of organizational-level consequences), we could undertake a survey of cybersecurity professionals to determine the extent that policy non-compliance actually leads to cybersecurity incidents (relative to other sources, such as unpatched systems). For Conjecture 2 (variance in policy quality makes for an unreliable dependent variable), we could undertake a qualitative comparison, perhaps using linguistic analysis, to compare the clarity and readability of a variety of policies. For Conjecture 3 (variance in employee familiarity with policies makes for an unreliable dependent variable), we could conduct a survey of business users to determine when they last read their firm's cybersecurity policy and the extent to which they understood its content.

4. Conclusions

In this research commentary, we suggest that the prevailing emphasis on policy compliance in behavioral cybersecurity research is susceptible to several notable limitations that could lead to inaccurate research conclusions. Specifically, we assert that the link between policy compliance and organizational-level outcomes is ambiguous; that policies vary widely in terms of their clarity and completeness; and that employees have an inconsistent familiarity with their own organization's cybersecurity policies. In response, we advocate that future research adopts an increasingly risk-centric approach, namely a focus on insecure cybersecurity behavior, cybersecurity vulnerabilities, and actual incidents. Our aim is to encourage the continued refinement of cybersecurity research approaches that can extend our theoretical insights and provide useful, timely guidance for managers.

5. References

Aurigemma, S., & Mattson, T. (2019). Generally speaking, context matters: Making the case for a change from universal to particular ISP research. *Journal of the Association for Information Systems, 20*(12), 1700-1742.

Balozian, P., & Leidner, D. (2017). Review of IS security compliance: Toward the building blocks of an IS security theory. *The DATA BASE for Advances in Information Systems, 48*(3), 11-43.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation. *Computers & Security, 39*(Part B), 145-159.

Barlow, J. B., Warkentin, M., Ormond, D., & Dennis, A. R. (2018). Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. *Journal for the Association for Information Systems, 19*(8), 689-715.

Baskerville, R. L., & Siponen, M. (2002). An information security meta-policy for emergent organizations. *Logistics Information Management, 15*(5/6), 337-346.

Bauer, S., & Bernroider, E. W. N. (2017). From information security awareness to reasoned compliant action: Analyzing information security policy compliance in a large banking organization. *The DATA BASE for Advances in Information Systems, 48*(3), 44-68.

Boehm, J., Curcio, N., Merrath, P., Shenton, L., & Stähle, T. (2019). *The risk-based approach to cybersecurity*. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/The%20risk%20based%20approach%20to%20cybersecurity/The-risk-based-approach-to-cybersecurity.pdf

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523-548.

Burns, A. J., Roberts, T. L., Posey, C., Bennett, R. J., & Courtney, J. F. (2018). Intentions to comply versus intentions to protect: A vie theory approach to understanding the influence of insiders' awareness of organizational seta efforts. *Decision Sciences, 49*(6), 1187-1228.

Coetzee, P., & Lubbe, D. (2014). Improving the efficiency and effectiveness of risk-based internal audit engagements. *International Journal of Auditing, 18*, 115-125.

Cram, W. A., D'Arcy, J., & Proudfoot, J. G. (2019). Seeing the forest and the trees: A meta-analysis of the antecedents to information security policy compliance. *MIS Quarterly, 43*(2), 525-554.

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2017). Organizational information security policies: A review and research framework. *European Journal of Information Systems, 26*(6), 605-641.

Dinev, T., Goo, J., Hu, Q., & Nam, K. (2009). User behaviour towards protective information technologies: The role of national cultural differences. *Information Systems Journal, 19*(4), 391-412.

Doherty, N. F., Anastasakis, L., & Fulford, H. (2009). The information security policy unpacked: A critical study of the content of university policies. *International Journal of Information Management, 29*(6), 449-457.

Doherty, N. F., & Fulford, H. (2005). Do information security policies reduce the incidence of security breaches: An exploratory analysis. *Information Resources Management Journal, 18*(4), 21-39.

Farshadkhah, S., Van Slyke, C., & Fuller, B. (2021). Onlooker effect and affective responses in information security violation mitigation. *Computers & Security, 100*(-), 1-16.

Feng, G., Zhu, J., Wang, N., & Liang, H. (2019). How paternalistic leadership influences IT security policy compliance: The mediating role of the social bond. *Journal of the Association for Information Systems, 20*(11), 1650-1691.

Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *Computers & Security, 61*(-), 169-183.

Goel, S., & Chengalur-Smith, I. N. (2010). Metrics for characterizing the form of security policies. *Journal of Strategic Information Systems, 19*(4), 281-295.

Goel, S., Williams, K. J., Huang, J., & Warkentin, M. (2021). Can financial incentives help with the struggle for security policy compliance? *Information & Management, 58*(4), 1-12.

Goo, J., Yim, M.-S., & Kim, D. J. (2014). A path to successful management of employee security compliance: An empirical study of information security climate. *IEEE Transactions on Professional Communication, 57*(4), 286-308.

Grover, V., Lindberg, A., Benbasat, I., & Lyytinen, K. (2020). The perils and promises of big data research in information systems. *Journal of the Association for Information Systems, 21*(2), 268-291.

Gwebu, K. L., Wang, J., & Hu, M. Y. (2020). Information security policy noncompliance: An integrative social influence model. *Information Systems Journal, 30*(2), 220-269.

Harrington, S. J. (1996). The effect of codes of ethics and personal denial of responsibility on computer abuse judgements and intentions. *MIS Quarterly, 20*(3), 257-278.

Herath, T., & Rao, H. R. (2009). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106-125.

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

Hina, S., Selvam, D. D. D. P., & Lowry, P. B. (2019). Institutional governance and protection motivation: Theoretical insights into shaping employees' security compliance behavior in higher education institutions in the developing world. *Computers & Security, 87*(-), 1-15.

Howard, P. D. (2003). The security policy life cycle: Functions and responsibilities. In H. F. Tipton & M. Krause (Eds.), *Information security management handbook* (pp. 297-311). Auerbach Publications.

Hsu, J. S.-C., Shih, S.-P., Hung, Y. W., & Lowry, P. B. (2015). The role of extra-role behaviors and social controls in information security policy effectiveness. *Information Systems Research, 26*(2), 282-300.

Hwang, I., Kim, D., Kim, T., & Kim, S. (2017). Why not comply with information security? An empirical approach for the causes of non-compliance. *Online Information Review, 41*(1), 2-18.

IBM Security. (2021). *Ibm x-force threat intelligence report 2021*. https://www.ibm.com/security/data-breach/threat-intelligence

Jaeger, L., Eckhardt, A., & Kroenung, J. (2021). The role of deterrability for the effect of multi-level sanctions on information security policy compliance: Results of a multigroup analysis. *Information & Management, 58*(3), 1-14.

Jenkins, J. L., & Durcikova, A. (2013). What, i shouldn't have done that? : The influence of training and just-in-time reminders on secure behavior. Thirty-Fourth International Conference on Information Systems, Milan, Italy.

Jenkins, J. L., Durcikova, A., & Nunamaker Jr., J. F. (2021). Mitigating the security intention-behavior gap: The moderating role of required effort on the intention-behavior relationship. *Journal of the Association for Information Systems, 22*(1), 246-272.

Jeon, S., Son, I., & Han, J. (2020). Exploring the role of intrinsic motivation in ISSP compliance: Enterprise digital rights management system case. *Information Technology & People, 34*(2), 599-616.

Jeske, D., & van Schaik, P. (2017). Familiarity with internet threats: Beyond awareness. *Computers & Security, 66*(-), 129-141.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549-566.

Karlsson, F., Hedström, K., & Goldkuhl, G. (2017). Practice-based discourse analysis of information security policies. *Computers & Security, 67*(-), 267-279.

Kaspersky Lab. (2018). *Kaspersky lab survey: One-in-ten employees are aware of their organization's IT security policies*. Retrieved October 24, 2021 from https://usa.kaspersky.com/about/press-releases/2018_one-in-ten-employees-are-aware-of-their-organizations-it-security-policies

Moody, G. D., Siponen, M., & Pahnila, S. (2018). Toward a unified model of information security policy compliance. *MIS Quarterly, 42*(1), 285-331.

NIST. (2017). *An introduction to information security*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-12r1.pdf

Ormond, D., Warkentin, M., & Crossler, R. E. (2019). Integrating cognition with an affective lens to better understand information security policy compliance. *Journal for the Association for Information Systems, 20*(12), 1794-1843.

Paananen, H., Lapke, M., & Siponen, M. (2020). State of the art in information security policy development. *Computers & Security, 88*(-), 1-14.

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, D. T. (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. (2020). Employees' behavior in phishing attacks: What individual, organizational, and technological factors matter? *Journal of Computer Information Systems, Forthcoming*, 1-12.

Sharma, S., & Warkentin, M. (2019). Do i really belong?: Impact of employment status on information security policy compliance. *Computers & Security, 87*(-), 1-12.

Silic, M., & Lowry, P. B. (2020). Using design-science based gamification to improve organizational security training and compliance. *Journal of Management Information Systems, 37*(1), 129-161.

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

Siponen, M., & Vance, A. (2014). Guidelines for improving the contextual relevance of field surveys: The case of information security policy violations. *European Journal of Information Systems, 23*(3), 289-305.

Stahl, B. C., Doherty, N. F., & Shaw, M. (2012). Information security policies in the UK healthcare sector: A critical evaluation. *Information Systems Journal, 22*(1), 77-94.

Straub, D. W. (1990). Effective IS security: An empirical study. *Information Systems Research, 1*(3), 255-276.

Straub, D. W., & Nance, W. D. (1990). Discovering and disciplining computer abuse in organizations: A field study. *MIS Quarterly, 14*(1), 45-62.

Trang, S., & Nastjuk, I. (2021). Examining the role of stress and information security policy design in information security compliance behaviour: An experimental study of in-task behaviour. *Computers & Security, 104*(-), 1-15.

Vance, A., Anderson, B. B., Kirwan, C. B., & Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (eeg). *Journal of the Association for Information Systems, 15*(10), 679-722.

Verizon. (2021). *2021 data breach investigations report*. Verizon. https://www.verizon.com/business/resources/reports/dbir

Ward, P., & Smith, C. L. (2002). The development of access control policies for information technology systems. *Computers & Security, 21*(4), 356-371.

Weber, S. (2022). *Compete to communicate on cybersecurity*. Infosecurity Magaize. Retrieved May 19, 2022 from https://www.infosecurity-magazine.com/opinions/compete-to-communicate/

Whitman, M. E. (2008). Security policy: From design to maintenance. In D. W. Straub, S. E. Goodman, & R. Baskerville (Eds.), *Information security: Policy, processes, and practices* (pp. 123-151). M. E. Sharpe.

Wiant, T. L. (2005). Information security policy's impact on reporting security incidents. *Computers & Security, 24*(6), 448-459.

Yazdanmehr, A., & Wang, J. (2021). Can peers help reduce violations of information security policies? The role of peer monitoring. *European Journal of Information Systems, Forthcoming*. https://doi.org/10.1080/0960085X.2021.1980444

Yazdanmehr, A., Wang, J., & Yang, Z. (2020). Peers matter: The moderating role of social influence on information security policy compliance. *Information Systems Journal, 30*(5), 791-844.

Yoo, C. W., Sanders, G. L., & Cerveny, R. P. (2018). Exploring the influence of flow and psychological ownership on security education, training and awareness effectiveness and security compliance. *Decision Support Systems, 108*(-), 107-118.