Received: 17 May 2022 | Revised: 8 June 2023 | Accepted: 5 July 2023

DOI: 10.1111/isj.12460

RESEARCH ARTICLE

WILEY

'What a waste of time': An examination of cybersecurity legitimacy

W. Alec Cram[1] | John D'Arcy[2]

[1]School of Accounting & Finance, University of Waterloo, Waterloo, Canada

[2]Lerner College of Business and Economics, University of Delaware, Newark, Delaware, USA

Correspondence
W. Alec Cram, School of Accounting & Finance, University of Waterloo, 200 University Ave West, Waterloo, ON N2L 3G1 Canada.
Email: wacram@uwaterloo.ca

Funding information
CPA Ontario; CPA Ontario Centre for Performance Management Research and Education; Social Sciences and Humanities Research Council of Canada, Grant/Award Number: 435-2021-0437

Abstract

Managers who oversee cybersecurity policies commonly rely on managerial encouragement (e.g., rewards) and employee characteristics (e.g., attitude) to drive compliant behaviour. However, whereas some cybersecurity initiatives are perceived as reasonable by employees, others are viewed as a 'waste of time'. This research introduces employee judgements of *cybersecurity legitimacy* as a new angle for understanding employee compliance with cybersecurity policies over time. Drawing on theory from the organisational legitimacy and cybersecurity literature, we conduct a three-wave survey of 529 employees and find that, for each separate wave, negative legitimacy judgements mediate the relationship between management support and compliance, as well as between cybersecurity inconvenience and compliance. Our results provide support for cybersecurity legitimacy as an important influence on employee compliance with cybersecurity initiatives. This is significant because it highlights to managers the importance of not simply expecting compliant employee behaviour to follow from the introduction of cybersecurity initiatives, but that employees need to be convinced that the initiatives are fair and reasonable. Interestingly, we did not find sufficient support for our expectation that the increased likelihood of a cybersecurity incident will moderate the legitimacy-policy compliance relationship. This result suggests that the legitimacy perceptions

of employees are unyielding to differences in the risk characteristics of the cybersecurity incidents facing organisations.

KEYWORDS
compliance, cybersecurity, inconvenience, legitimacy, management support, policy

1 | INTRODUCTION

The organisational consequences of cybersecurity incidents are well established (Ponemon Institute, 2020; Verizon, 2020), as is the increasing attention paid by managers to encourage employees to comply with the policies that guide their cybersecurity-related behaviour (Balozian et al., 2019; Cram et al., 2019). Despite initiatives that aim to protect the organisation, employees vary the extent of their cybersecurity compliance (and non-compliance) behaviours due to a variety of factors, including managerial encouragements (e.g., rewards, punishments) and their own personal traits (e.g., attitude, ethics) (Moody et al., 2018). However, the inconsistent policy compliance behaviour of employees remains a cause of frustration to organisations that bear the financial, reputational, and regulatory costs of successful cybersecurity attacks.

One plausible explanation for this ongoing variability in employees' cybersecurity policy compliance behaviour lies neither in managerial actions nor individual traits, but rather with the ongoing perceptions, beliefs, and judgements made by employees regarding the cybersecurity initiatives themselves (Cram et al., 2017; Karjalainen et al., 2019). For example, following company guidelines to avoid the use of cloud-based storage services (e.g., Dropbox) may be deemed a reasonable practice to an executive at a bank that faces a high probability of cyber-attack, but that same requirement could be judged as unreasonable to a junior employee where the risks are much lower. It would seem realistic that both employees undertake an individual evaluation of the appropriateness of the cloud-based storage usage rule and then act according to this viewpoint. Despite past calls for research that investigates how employees undertake such legitimacy judgements regarding cybersecurity initiatives (e.g., Cram et al., 2017; Li et al., 2014), there has been very little research conducted on the phenomenon to date. Legitimacy[1] refers to the judgements made by employees that organisational properties and behaviours are fair, proper, and appropriate (Alge et al., 2006; Suchman, 1995).

This study draws on theory from the organisational legitimacy and the cybersecurity policy compliance literature to investigate the antecedent factors that are associated with employee judgements of the legitimacy of cybersecurity behaviours and actions, as well as the behavioural consequences of those judgements. We ground our study in Bitektine and Haack's (2015) perception-judgement-action model of micro-level legitimacy, which argues that organisations display properties and behaviours that are *perceived* by employees, who then make *judgements* on the (positive or negative) legitimacy of those properties, and then undertake resulting *actions*. In applying this model within the context of an organisation's cybersecurity activities, we focus on two key employee perceptions. First, we consider how employees perceive the behaviour and actions of managers in facilitating cybersecurity activities, referred to as top management support. Second, we consider how employees perceive the cybersecurity rules and guidelines implemented by management, referred to as cybersecurity inconvenience. Distinct from past research that

[1]We acknowledge that some ambiguity exists regarding the terminology used to describe positive versus negative legitimacy. In this research, we follow the perspective of Tost (2011), who argues that legitimacy can be thought of as 'a continuous variable, with values above a neutral point constituting positive legitimacy judgements and values below a neutral point constituting negative legitimacy judgements (i.e., illegitimacy)' (p. 701). As such, we use the term legitimacy as an umbrella term that is inclusive of both positive judgements (e.g., a behaviour is fair, proper, and appropriate), as well as negative judgements (e.g., a behaviour is unfair, improper, and inappropriate). When we use the term negative legitimacy, we refer only to negative judgements. This approach is consistent with past research, including by Bitektine and Haack (2015), Kraatz and Zajac (1996), and Sanders and Tuschke (2007).

has investigated a direct link between management support and compliance (e.g., Ifinedo, 2016; Shropshire et al., 2015) or inconvenience and compliance (e.g., Hwang et al., 2017; Ifinedo, 2012; Vance et al., 2012), we examine a new theoretical model that predicts that these employee perceptions will first shape negative legitimacy judgements of the security initiatives, which will then influence behavioural compliance. To further contextualise our understanding of legitimacy to the cybersecurity context, we also predict that judgements on the increased probability of a security incident will weaken the relationship between negative legitimacy judgements and compliance, thus acting as a form of judgement suppression. That is, an employee may view the password policy to place an unreasonable burden on them, but due to the high perceived risk of a security breach, they will still decide to comply.

We undertook a three-wave survey using repeated measures of 529 employees that was conducted over a 7-month period. Our aim was to answer two research questions: (1) *To what extent does cybersecurity legitimacy mediate the relationship between (a) top management support and cybersecurity policy compliance; and (b) cybersecurity inconvenience and cybersecurity policy compliance?* (2) *To what extent does judgement on the probability of a cybersecurity incident moderate the relationship between cybersecurity legitimacy and cybersecurity policy compliance?*

Our results support the prediction that cybersecurity legitimacy acts as a significant mediator between top management support and compliance, as well as cybersecurity inconvenience and compliance. This is a key contribution to the ongoing refinement of behavioural cybersecurity theory in that it suggests that employees make independent judgements on the legitimacy of organisational properties/behaviours, and then take action based on their judgements. Although past research has established direct links between organisational behaviours such as top management support and compliance (which our study confirms), our results are distinct in that we demonstrate the *indirect* consequences of organisational properties and behaviours on individual-level compliance behaviour via cybersecurity legitimacy perceptions. Specifically, we show that cybersecurity legitimacy represents a mediating link between inconvenience and policy compliance, but note that a significant, direct relationship was not found between inconvenience and compliance. As well, our results point to a complementary link between management support and policy compliance (i.e., there was both a significant, direct and indirect relationship). This is notable because it highlights to managers the importance of not simply expecting compliant employee behaviour to follow from the introduction of cybersecurity initiatives, but that employees need to be convinced that the initiatives are fair and reasonable. Surprisingly, we did not find sufficient support for the hypothesis that judgement of the increased likelihood of a cybersecurity incident will moderate the legitimacy-policy compliance relationship. This result adds valuable insight to the discourse on compliance behaviour by suggesting that the legitimacy perceptions of employees are unyielding to differences in the risk characteristics of the cybersecurity incidents facing organisations. Our finding is of particular concern for organisations because it suggests that if employees do not judge cybersecurity initiatives to be legitimate, their corresponding level of policy compliance will remain unaffected, even if they are aware that an incident is highly likely to occur. In effect, their negative legitimacy judgement outweighs their awareness of high probability incidents. Practically, this challenges existing assumptions about the effectiveness of just-in-time warnings or reminders from IT pertaining to evolving trends may influence employees to behave in a more compliant way.

2 | CONCEPTUAL FOUNDATIONS

This study draws on past research from two foundational areas: organisational legitimacy and cybersecurity policy compliance. We begin by providing an overview on the concept of legitimacy and its role in institutions. Next, we outline the past use and remaining opportunities in the cybersecurity literature to investigate legitimacy-related issues.

2.1 | Organisational legitimacy

Institutional theory considers a variety of issues pertaining to value creation, order, structure, belief systems, and social reality (Meyer & Rowan, 1977; Scott, 1987). Within the context of organisations, institutional theory can

provide insights regarding the behaviour of employees, including the processes that influence behaviour changes over time (Deephouse & Suchman, 2008; Suddaby et al., 2017). One line of inquiry within the study of institutional theory pertains to legitimacy, which is primarily applied in an organisational context (Tost, 2011) and refers to the 'perception or assumption that the actions of an entity are desirable, proper, or appropriate within some socially constructed system of norms, values, beliefs, and definitions' (Suchman, 1995, p. 574). Past research has applied the concept widely, considering both macro applications (e.g., how a company as a whole can gain and maintain legitimacy), as well as microlevel applications pertaining to individual employee perspectives (Bijlsma-Frankema & Costa, 2010; Bitektine & Haack, 2015; Suddaby et al., 2017). For example, a recent study by Hsu et al. (2022) examines how a client's perceived legitimacy of IT vendors impacts outsourcing performance. Fundamentally, the study of legitimacy focuses on 'addressing the normative and cognitive forces that constrain, construct, and empower organizational actors' (Suchman, 1995, p. 571).

In the context of this study, we are interested in how legitimacy can be applied to better understand the institutional forces that influence employee behaviour associated with cybersecurity policies. As noted, such a perspective has largely been neglected in the cybersecurity literature to date. Since one stream of legitimacy research focuses on the evaluation of organisational practices at a micro level (Hoefer & Green, 2016; Suddaby et al., 2017), we leveraged this body of work as a foundation for our study. Specifically, three steps are conceptualised as representing the legitimacy process undertaken by individual employees (Bitektine & Haack, 2015; Tost, 2011): perceptions, judgements, and actions. First, organisations display properties and behaviours (via the combined actions of management and owners) that are *perceived* by employees. For example, if an organisation's leadership team enters into a merger with another firm or decides to lay off staff, employees perceive that this behaviour takes place. Second, employees make *judgements* on the organisational properties and behaviours in terms of whether they are consistent, fair, and proper (Suddaby et al., 2017). This assessment can range from individuals concluding that a behaviour constitutes positive legitimacy (e.g., the merger is appropriate since the acquired firm has values consistent with the acquiring firm) or negative legitimacy (i.e., it is inconsistent with the firm's norms to lay off staff in order to increase profits) (Tost, 2011). Finally, employees determine the appropriate *actions* that they will undertake as a result of their judgement. This can include both substantive actions (e.g., voicing public support for the merger, publicly protesting the layoffs), as well as 'judgement suppression', which refers to individuals who choose not to undertake any observable action (e.g., not acting on views that the layoffs are unwarranted due to fear of management sanctions) (Bitektine & Haack, 2015). Overall, this perception-judgement-action process provides a valuable lens for understanding the relationships between the initiatives undertaken by organisations and the consequences this has on employee behaviour. We apply the framework in the context of cybersecurity policy compliance in the following section.

2.2 | Cybersecurity policy compliance: A legitimacy perspective

Research examining employee compliance with organisational cybersecurity policies has an extensive history and draws on a range of theoretical foundations. Past studies have investigated the compliance antecedents originating from deterrence theory (e.g., certainty and severity of sanctions) (Chen et al., 2012; D'Arcy et al., 2009), neutralisation theory (e.g., denial of responsibility) (Siponen & Vance, 2010), protection motivation theory (Menard et al., 2017; Schuetz et al., 2020), and the theory of planned behaviour (e.g., costs and benefits of compliance) (Bulgurcu et al., 2010), among others. However, despite this variety of explanatory factors, past research continues to point to inconsistent findings and unexplained variance in attempts to predict employee compliance with cybersecurity policies (Cram et al., 2019; Menard et al., 2017).

As described in the preceding section, the properties and behaviour of organisations are perceived, judged, and acted upon by employees. One particularly important behaviour is the organisation's initiatives pertaining to cybersecurity threats, such as the implementation of policies and guidelines. We suggest that such organisational behaviours are perceived and then judged in terms of their legitimacy by employees, and then acted upon via compliance

(or non-compliance). Although we recognise that positive legitimacy judgements could be associated with positive employee actions, we are particularly interested in the negative legitimacy judgements that could weaken cybersecurity policy compliance. In the cybersecurity context, negative legitimacy represents an employee judgement that the cybersecurity behaviours and properties of an organisation are unfair, improper, or inappropriate within an employee's system of norms, values, and beliefs. Refer to Table 1 for a listing of related definitions.

A limited amount of past work has been undertaken in the behavioural cybersecurity literature on legitimacy-related issues, despite past calls for more research by Cram et al. (2017) and Li et al. (2014). One exception is an early example from Son (2011), who considers the source of employee motivations as an explanation for why employees violate cybersecurity policies. As part of the study's operationalization of intrinsic motivations, perceived legitimacy was found to have a significant, positive relationship with cybersecurity policy compliance. As well, Lowry et al. (2015), draw on elements of fairness theory[2] to explain the deliberate misuse of computing assets by insiders, but reveal inconsistencies in the direct relationships (i.e., two of three hypothesised paths were not deemed significant). More recently, Yazdanmehr et al. (2020) examine the direct link between a self-regulatory approach (consisting of legitimacy and value congruence constructs) and cybersecurity policy compliance. The results of the study highlight a significant, positive relationship between the constructs.

Interestingly, both Son (2011) and Yazdanmehr et al. (2020) measure legitimacy using an adapted instrument from Tyler and Blader (2005), which primarily focuses on employee judgements regarding the acceptability of violating a cybersecurity policy. For example, measurement items include the following: people should support their organisational security policy; it is wrong to break an organisational security policy; and an employee should accept the organisational security policy. Although we agree that this focus provides insights into the behavioural *actions* an employee might take, we suggest that it stops short of considering the *perceptions* and *judgements* of the organisation's cybersecurity properties and behaviours, and thus provides an incomplete view of the legitimacy concept in the cybersecurity realm.

TABLE 1 Key definitions.

Legitimacy element	Cybersecurity construct	Definition
Perceptions	Top management support	The behaviour and actions of managers in facilitating cybersecurity activities (Hu et al., 2012; Liang et al., 2007).
	Cybersecurity inconvenience	The extent that employees perceive the cybersecurity rules and guidelines implemented by management to impede their productivity and efficiency at work (Bulgurcu et al., 2010).
Judgements	Negative cybersecurity legitimacy	The judgement that the cybersecurity behaviours and properties of an organisation are unfair, improper, or inappropriate within an employee's system of norms, values, and beliefs (Alge et al., 2006; Suchman, 1995).
	Probability of a cybersecurity incident	An employee's assessment of the likelihood of a cybersecurity incident that results in the loss of assets (Herath & Rao, 2009).
Actions	Cybersecurity policy compliance	The extent that an employee complies with the cybersecurity policy guidelines (D'Arcy & Lowry, 2019).

[2]We acknowledge that aspects of fairness are considered in both fairness theory and organisational legitimacy research. However, whereas fairness theory focuses on a person's attribution of blame towards an individual for actions that threaten material or psychological well-being (Folger & Cropanzano, 2001) (e.g., it is unfair that my manager asks me to attend cybersecurity training, because I find it boring and frustrating), organisational legitimacy encompasses a broader, more complex set of judgements that extend beyond the threat to one's well-being by also considering the behaviour relative to the perceiver's norms, values, and beliefs (Alge et al., 2006) (e.g., it is not legitimate that my manager asks me to attend cybersecurity training because the materials are out of date and do not provide the necessary guidance for me to adequately protect the firm's IT assets). In short, legitimacy judgements are formed in terms of an individual's system of norms, values, and beliefs, of which fairness represents one contributing (but only partial) factor.

The study of legitimacy within a cybersecurity context provides a promising opportunity for valuable new insights into employee behaviour and we suggest that several promising lines of inquiry remain untapped. First, we believe there is an opportunity to reorient the focus of legitimacy research in cybersecurity towards the cybersecurity properties and behaviours of the *organisation*, which asks questions such as 'Is the password policy implemented by the organization fair and appropriate?' Doing so is distinct from past work by Son (2011) and Yazdanmehr et al. (2020), who focus instead on the appropriateness of the *employee's compliance behaviour*. In doing so, we can better distinguish if the rationale for the employee's action is inherently a matter of attitude and personal ethics or if compliance actions are also driven by the specific nature of the organisation's cybersecurity properties and behaviours. Second, there has been no work to date that we are aware of that identifies the specific organisational cybersecurity properties and behaviours that are perceived by employees and then subsequently assessed for legitimacy. Clarifying these constructs could help establish a theoretical model of the antecedents to legitimacy judgements. Third, we are also unaware of any research that studies the 'judgement suppression' phenomenon described above, where an employee deems an organisational behaviour to not be legitimate, but decides not to undertake any observable action. There is an opportunity to investigate if there are circumstances within the context of cybersecurity where an employee may judge a cybersecurity policy to not be legitimate, but still chooses to comply with it. Finally, since legitimacy is an iterative, multistep process (Bitektine & Haack, 2015; Tost, 2011), it remains unclear how legitimacy perceptions, judgements, and actions related to cybersecurity initiatives may change over time. This represents an opportunity to investigate the extent that legitimacy relationships fluctuate or remain stable over time, which can lay the groundwork for future research that investigates the sources of any potential temporal instability in this context.

3 | RESEARCH MODEL

Our research model (see Figure 1) builds on and integrates the legitimacy concepts and the cybersecurity policy compliance elements outlined above. We aim to extend theory and practice in several unique directions by: (a) Orienting the legitimacy focus on organisational properties and behaviours related to cybersecurity; (b) investigating the specific types of organisational properties and behaviours that are perceived and judged for legitimacy; and (c) examining circumstances where employees may undergo judgement suppression related to their legitimacy judgements. In doing so, we advance theoretical understanding of the relationships between top management support and cybersecurity inconvenience——two known predictors of cybersecurity policy compliance——by explaining cybersecurity legitimacy

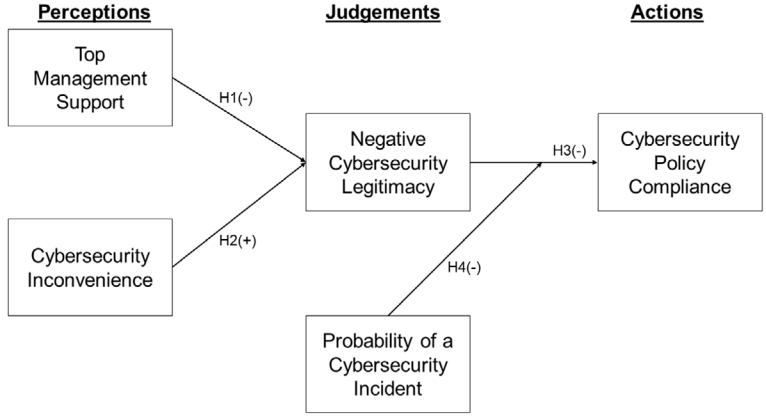


FIGURE 1 Research model.

as an underlying mechanism to these relationships. As we note above, our interest is on the harmful actions that could stem from legitimacy judgements and as such, we focus specifically on negative legitimacy judgements.

3.1 | Top management support, legitimacy, and policy compliance

Top management support refers to the behaviour and actions of managers in facilitating cybersecurity activities (Hu et al., 2012; Liang et al., 2007). Past research has identified links between top management support and compliance, most commonly as either a direct relationship (e.g., Ifinedo, 2016; Shropshire et al., 2015) or via security culture/climate (e.g., Chan et al., 2005; D'Arcy & Greene, 2014; Goo et al., 2014). However, we posit that compliance behaviour is not only influenced by the existence of strong management support, but that employees will also judge the legitimacy of that supporting behaviour, in terms of its desirability and appropriateness, before deciding to comply with organisational guidelines. That is, employees do not simply comply with security initiatives because management says they are important; rather, employees make independent judgements on what management communicates and then determines if they are compelling and convincing. Based on this determination, they comply (or not).

Past research argues that management communications and behaviours are key factors in shaping legitimacy judgements, whereby employees actively process information received by management and make judgements on how to act (Hoefer & Green, 2016; Tost, 2011). Here, managers may present arguments that aim to reinforce the legitimacy of an organisational practice, while employees receive that communication, interpret it, and make sense of the arguments (Hoefer & Green, 2016; Suddaby & Greenwood, 2005; Tost, 2011). Since legitimacy is a fundamental mechanism for driving organisational change, managers who can advocate equitable and reasonable strategies to employees are more likely to be successful attaining their targets (Feng et al., 2019; Narayanaswamy et al., 2013; Suddaby & Greenwood, 2005). As such, where plans for cybersecurity initiatives are presented to employees in a way that is consistent with their norms and values, managers expect that the likelihood of employee resistance will be diminished, whereas negative legitimacy will be associated with non-compliance (Tyler & Blader, 2005). This view is supported by Hu et al. (2012), who argue that employee beliefs tend to be influenced by observations of top management behaviour. They note that, 'by championing the new initiatives, programs, or policies through articulating a clear vision and strategy and setting the goals and measures about the initiatives, programs, or policies, top management renders legitimacy' (p. 628). Other work by Johnston et al. (2019) argues that where the language used by managers in describing cybersecurity initiatives aligns with the norms of an employee, they will be more likely to be persuaded to follow the recommended guidelines. Therefore, by enhancing legitimacy (and thus weakening negative legitimacy) through their cybersecurity actions, managers can encourage compliance with the cybersecurity activities. However, where managerial actions are not viewed as legitimate by employees, requests to perform additional work in order to comply with the cybersecurity initiatives are expected to be met with resistance (Hu et al., 2012). Based on these arguments, we propose H1:

> **H1.** Negative cybersecurity legitimacy mediates the positive relationship between top management support and cybersecurity policy compliance.

3.2 | Cybersecurity inconvenience, legitimacy, and policy compliance

Cybersecurity inconvenience refers to the extent that employees perceive the cybersecurity rules and guidelines implemented by management to impede their productivity and efficiency at work. The link between cybersecurity inconvenience (or related concepts such as work impediment and response cost) and policy compliance has been studied in past literature, most commonly as either a direct relationship (e.g., Hwang et al., 2017; Ifinedo, 2012; Vance et al., 2012) or mediated by attitude (e.g., D'Arcy & Lowry, 2019; Herath & Rao, 2009). However, we are not

aware of past work that has studied the relationship between inconvenience and legitimacy. In this context, we suggest that cybersecurity initiatives could be viewed by employees as a type of 'symbolic management', that is, initiatives that are undertaken by the organisation to appear to adequately attend to stakeholder expectations around cybersecurity risks but that actually conceal who is responsible for completing the necessary activities (Ashforth & Gibbs, 1990). For example, if the organisation espouses the importance of cybersecurity but then places an undue burden of following cybersecurity rules on employees, then those employees may increasingly judge the broader initiative to not be legitimate. This view is consistent with Long et al. (2011), who suggest that employees are most attuned to judging managerial rules when it is most relevant to their own success at work. Where the tasks are easy to follow, past research suggests that compliance is likely (Pahnila et al., 2007). However, in the case of inconvenient cybersecurity activities, employees may not deem them as legitimate on the basis that they have a negative impact on efficiency and productivity, which will be detrimental to their overall work performance. In part, this negative legitimacy judgement could be a function of the limited autonomy offered to employees regarding cybersecurity activities. Since many cybersecurity policy guidelines are highly prescriptive in terms of acceptable behaviours (i.e., an employee either complies or violates a rule), this lack of flexibility could leave employees feeling a lack of autonomy. Since past research points to autonomy as a key source of legitimacy (Bijlsma-Frankema & Costa, 2010), it would follow that the diminished autonomy stemming from inconvenient cybersecurity requirements may also be associated with negative legitimacy. Both Besnard and Arief (2004) and Bulgurcu et al. (2010) support this view by finding that where employees conclude that cybersecurity tasks will inhibit their work, they will be less inclined to comply with the regulations. Similarly, Ormond et al. (2019) find a link between cybersecurity tasks that are frustrating and the violation of policies. Based on these arguments, we suggest H2:

> **H2.** Negative cybersecurity legitimacy mediates the negative relationship between cybersecurity inconvenience and cybersecurity policy compliance.

3.3 | Legitimacy, incident probability, and compliance

Where an employee makes the judgement that an organisational behaviour or property is legitimate, it is increasingly likely that the employee 'will accept and comply with it' (Bijlsma-Frankema & Costa, 2010, p. 402); in contrast, where a behaviour or property is not judged to be legitimate, employees will comply to a lesser degree, in effect punishing the organisation for undertaking an activity they believe to be improper (Ormond et al., 2019; Schnedler & Vadovic, 2011). Past research has found links between legitimacy and compliance (e.g., Kraatz & Zajac, 1996; Son, 2011; Yazdanmehr et al., 2020) and broadly found that 'organizational practices that lead employees to view management as legitimate is another judgement that will also encourage rule following' (Tyler & Blader, 2005, p. 1145).

However, when an employee has judged an organisational property or behaviour to not be legitimate, we suggest that the employee's level of compliance could interact with other factors. Specifically, we argue that the corresponding negative relationship with compliance is likely to be dampened (i.e., there will be a weakened relationship between negative legitimacy and compliance) in cases where the employee expects that a security incident is probable. That is, even if an employee judges a policy not to be legitimate, if they also believe a cybersecurity incident is likely to occur due to high-risk external threats, they may still decide to comply despite their view that the policy is unreasonable. This is consistent with Bitektine and Haack's (2015) argument that some employees will supress their judgements and not act as they normally might (in this case, with policy non-compliance) due to the potential for social or personal consequences. Past research suggests that such judgement suppression is a result of attempting to avoid possible sanctions (Kuran, 1987), social disapproval from peers (Willer et al., 2009), or because acting in line with the legitimacy judgement is viewed as being futile (Kuran, 1995). Where a cybersecurity incident is seen as being imminent, employees may feel pressured to comply with security regulations as a means to avoid being responsible for contributing to an event would be detrimental to themselves and the organisation

(Kahneman & Tversky, 1979). That is, the potentially negative consequences of violating the policy may be deemed greater——in cases where attacks are more likely——than the benefits they might reap (e.g., gained efficiency or productivity). On this basis, we suggest H3 and H4:

H3. Employees who judge cybersecurity activities to not be legitimate will comply less with cybersecurity policies.

H4. The judgement of increased probability of a cybersecurity incident dampens the negative relationship between negative cybersecurity legitimacy and cybersecurity policy compliance.

4 | METHODOLOGY

In order to demonstrate the consistency of our model relationships beyond a single point in time, we designed a series of surveys that measured our model constructs at three separate times (each separated by 3 months) over a 7-month period. By doing so, we help counter the common method variance (CMV) concerns raised by Podsakoff et al. (2003), who suggest that when '…measures are taken at the same time in the same place, they may share systematic covariation because this common measurement context may (a) increase the likelihood that responses to measures of the predictor and criterion variables will co-exist in short-term memory, (b) provide contextual cues for retrieval of information from long-term memory, and (c) facilitate the use of implicit theories when they exist' (p. 885). With respect to these CMV-related concerns, as we later show in our results, the significant relationships we found are not bound to a single point in time. We began with a pre-screening participant survey, followed by three waves of data collection, where each wave consisted of two separate surveys (i.e., seven total surveys were completed by participants). We describe the details of the approach below.

4.1 | Survey instrument and data collection

Survey participants were recruited via Prolific Academic, an online crowdsourcing data collection organisation specialising in behavioural research. Prolific is well regarded for its reliable access to niche participant groups (e.g., employees of organisations with a cybersecurity policy), high quality data, international participants, and strong retention rates for multi-wave studies (Kothe & Ling, 2019; Palan & Schitter, 2018; Peer et al., 2017). Data collected in this manner grants anonymity to participants and provides access to a wide range of individuals (Lowry & Moody, 2015). The survey was hosted online using the Qualtrics survey software, and data were collected during the period of April–November 2020.

To test our research model and hypotheses, we developed a survey instrument using measurement items derived from existing scales that have been shown to have good psychometric properties in earlier studies. The items used for measuring top management support were derived from Hu et al. (2012). For cybersecurity inconvenience, we adapted items from Bulgurcu et al. (2010). Negative cybersecurity legitimacy was assessed using items from Alge et al. (2006) and Semmer et al. (2010). Finally, to assess survey participants' cybersecurity policy compliance, we used a combination of items from D'Arcy and Lowry (2019) and items derived from Schoorman and Mayer (2008). Both sets of items are self-reports, but the items derived from Schoorman and Mayer (2008) ask participants to rate their supervisor's opinion of their cybersecurity policy compliance (i.e., degree to which the supervisor thinks the participant engages in cybersecurity policy compliance). Hence, these additional items provide a surrogate for supervisor evaluations of cybersecurity policy compliance and thus help counter concerns about the assessments of this behaviour coming from a single source (Schoorman & Mayer, 2008). All constructs were measured reflectively with multiple items and rated on 7-point Likert scales, using 'strongly

disagree' and 'strongly agree' anchors. To account for alternative explanations, we collected data during the first survey on a range of demographic variables, covering both personal information (age, gender, education, country of residence) and work-related information (income, company size). An overview of all construct items is provided in Appendix A.

We pre-tested our survey instrument with five experienced scholars. Minor changes to the wording and flow of our survey resulted from this feedback. Our data collection started with a pre-screening survey that aimed to exclude participants who were not in a position to answer the main survey questions due to the nature of their employment. Using a combination of standard pre-screening criteria in Prolific and a short survey, we identified participants who met seven criteria. All participants were: (1) employed full time; (2) users of technology at work more than once per day; (3) fluent in English; (4) residents of either the USA or UK; (5) employed in an organisation with a cybersecurity policy; (6) employed at an organisation that conducts cybersecurity activities; and (7) employed in a role outside the IT department. The pre-screening survey was sent to Prolific members in late April 2020, and 2331 completed surveys were returned. Of these, 1479 participants met all of our criteria and qualified for the main survey. Refer to Table 2 for details of the data collection timing and quantity of survey responses.

The main survey data were collected over three waves, with each wave consisting of two separate surveys. We chose to divide each survey into two sections to reduce concerns surrounding CMV (Podsakoff et al., 2003). This design allowed us to avoid conceptual dependence between sets of questions (Addas & Pinsonneault, 2018) and temporally separate some of the independent and dependent variables for each wave of the data collection (Karahanna et al., 2018; Rowmanow et al., 2018). For the first survey in each wave, only the Part A questions (top management support, control variables) were asked, while the second survey contained questions from only Part B (inconvenience, legitimacy, compliance). Participants had 7 days to complete the first survey and 7 days to complete the second survey from each wave. The surveys for waves 2 and 3 were only sent to participants who had completed preceding surveys and passed the quality check criteria (each of the main surveys included two unique attention checks). A total of 180 participants failed an attention check at some point in the study (104 in wave 1, 60 in wave 2, and 28 in wave 3); these data were excluded from the analysis on the basis that they were unreliable.

In order to check for potentially systematic differences in participant attrition (e.g., employees who completed the survey in wave 1 but dropped out in wave 2 or 3), we followed the guidelines of Goodman and Blum (1996) by assessing the presence of non-random sampling, the effects of non-random sampling on means, the effects of non-random sampling on variances, and the effects of non-random sampling on the relationships among variables. We found some weak evidence that those who reported lower top management support for security were more likely to stay on for waves 2 and 3, but systematic differences in participant attribution were not detected for any of the other study variables.

TABLE 2 Survey data collection timing.

Activity	Survey questions	Timing	Surveys sent	Responses received	Total usable responses
Participant screening	Screening	20–30 April	16 265	2331	1479
Survey wave 1	Part A	1–7 May	1479	1049	969
	Part B	8–14 May	969	904	880
Survey wave 2	Part A	1–7 August	880	736	709
	Part B	8–14 August	709	655	622
Survey wave 3	Part A	1–7 November	622	566	554
	Part B	8–15 November	554	545	529

Survey waves took place in 3-month intervals, beginning in May, August, and November. Past commentators advise that care be taken in determining the length of time between data collection in multi-wave research. Because one of our research objectives was to assess the consistency of our model relationships, we chose a 3-month interval to allow for the introduction of potential variances into our study context. A total of 529 participants completed the pre-screening survey and all six main surveys. Please refer to Appendix B for a summary of demographic details.

4.2 | Measurement model assessment

To transform our research model into a structural equation model, we used covariance-based structural equation modelling (CB-SEM) using IBM SPSS Amos 26.0 (West Yorkshire, UK). Separate models were created for each of the three data collection waves. We first conducted a confirmatory factor analysis (CFA) of the measurement model constructs. The composite reliability for each construct exceeded the recommended 0.70 (Nunnally & Bernstein, 1994) and the recommended 0.50 (Fornell & Larcker, 1981) for average variance extracted (AVE). As such, these values indicate good reliability and convergent validity. Discriminant validity was assessed using the heterotrait–monotrait (HTMT) ratio, which has been advocated as a robust technique for CB-SEM (Franke & Sarstedt, 2019; Hair et al., 2017; Voorhees et al., 2016). Our HTMT results found that all values were within the strict 0.85 cutoff (Henseler et al., 2015), which indicates adequate discriminant validity. Table 3 shows the measurement quality results from the confirmatory factor analysis. Construct correlations are presented in Table 4, while item loadings and Cronbach's alpha results are noted in Appendix C.

4.3 | Common method variance

Although we took certain steps to alleviate concerns about CMV in our data (i.e., repeated measures, supervisor perspective in measuring cybersecurity policy compliance and temporal separation of certain independent and dependent variables for each survey wave), it is still a potential risk. To further reduce this risk, we used numerous procedural remedies during the design of our survey instrument, such as keeping questions simple and concise; maintaining conceptual dependence between dependent and independent variables; using randomised items; and reiterating the confidentiality of responses to participants (Addas & Pinsonneault, 2018; Podsakoff et al., 2003). We also conducted several post hoc analyses. First, extremely high construct correlations are a possible indicator of CMV (Podsakoff et al., 2003). The highest correlation between constructs is 0.658 (see Table 4), which is well below the suggested threshold of 0.90 (Bagozzi et al., 1991; Pavlou et al., 2007). Second, we performed a full collinearity test, which is considered an effective test for the identification of CMV (Kock, 2015). Although this test was intended for partial least squares methods, the principles also apply to covariance-based methods (Gaskin, 2020). We calculated the VIF values for all constructs and control variables included in our research model. All VIF values are clearly below the most conservative threshold of 3.3 (Hu & Bentler, 1999), with the highest value totalling 1.705. Third, we utilised the marker variable approach with an unmeasured latent factor (Lindell & Whitney, 2001). Specifically, we measured 'disposition to trust' using Gefen's five-item instrument (Gefen, 2000) as a theoretically unrelated factor in our model. Past research, such as Addas and Pinsonneault (2018), Cameron and Webster (2013), and Shao and Li (2022), have also used this construct as a marker variable. In Amos, we included the marker variable as a covariate of other factors in the model, then added an unmeasured latent factor, which partials out the variance shared by the marker and other factors (Gaskin, 2020; Williams et al., 2010). We conducted a chi-square difference test to compare the unconstrained model to a model where shared variances are constrained to be zero (i.e., no bias) and the significant result suggested the potential for bias. Therefore, we retained the common factor and marker factor in our imputed factor scores, which accounts for this bias in our causal modelling (i.e., testing the structural relationships) (Gaskin, 2020).

TABLE 3 Measurement quality from CFA.

Construct	Mean	SD	CR	MSV	MaxR(H)	AVE	√AVE
Wave 1							
MSUPPT_1	2.79	1.36	0.919	0.088	0.942	0.792	0.890
INCON_1	5.64	1.34	0.935	0.394	0.938	0.782	0.884
LEGIT_1	5.84	1.27	0.912	0.394	0.914	0.597	0.773
COMPLI_1	1.75	0.88	0.922	0.183	0.924	0.664	0.815
PROB_1	3.28	1.75	0.827	0.003	0.873	0.617	0.786
Wave 2							
MSUPPT_2	3.00	1.43	0.947	0.091	0.950	0.857	0.926
INCON_2	5.58	1.41	0.948	0.433	0.954	0.820	0.905
LEGIT_2	5.83	1.23	0.920	0.433	0.925	0.621	0.788
COMPLI_2	1.78	0.89	0.936	0.192	0.939	0.710	0.842
PROB_2	3.26	1.73	0.810	0.009	0.871	0.593	0.770
Wave 3							
MSUPPT_3	2.93	1.42	0.945	0.105	0.955	0.851	0.922
INCON_3	5.49	1.40	0.947	0.373	0.949	0.816	0.904
LEGIT_3	5.85	1.23	0.915	0.373	0.918	0.606	0.778
COMPLI_3	1.72	0.78	0.934	0.189	0.940	0.703	0.839
PROB_3	3.29	1.74	0.854	0.012	0.869	0.661	0.813

Abbreviations: AVE, average variance extracted; CR, composite reliability; MaxR(H), maximum reliability; MSV, mean squared variance; SD, standard deviation.

4.4 | Structural model assessment

The structural model was tested using IBM SPSS Amos 26.0. Again, separate models were constructed for each wave of data collection. We started by removing the covariances of the non-independent variables, then added the structural paths based on the hypotheses outlined above. We evaluated the structural model for goodness-of-fit with the data and found that the measurements were within the accepted cutoffs of greater than 0.95 for comparative fit index (Bentler, 1992; Hu & Bentler, 1999; Marsh et al., 2004), less than 0.08 for standardised root mean square residual (Hu & Bentler, 1999), less than 0.06 for root mean square error of approximation (Hu & Bentler, 1999), and greater than 200 for Hoelter's Critical N (Hoelter, 1983). Refer to Table 5 for details of the goodness-of-fit statistics.

IBM SPSS Amos 26.0 was also used to evaluate the mediation hypotheses (H1 and H2), the direct relationship hypothesis (H3), and the moderation hypothesis (H4). To evaluate the mediating role of legitimacy in the relationship between top management support and compliance (H1) and cybersecurity inconvenience and compliance (H2), we imputed the factor scores for the model constructs and conducted a test for indirect effects (Blunch, 2013; Kline, 2016). Amos reports direct effects (the unmediated relationship between two constructs), indirect effects (the mediated relationship between two constructs), and total effects (the sum of the direct and indirect effects). Where significant indirect effects are found, the mediating construct——in this case, legitimacy——is responsible for this influence (Gaskin, 2020). To test the direct effects of cybersecurity legitimacy on compliance (H3), we evaluated the results of the structural model. Finally, to test the moderating effects of the probability of a cybersecurity incident on the relationship between legitimacy and compliance (H4), we imputed the factor scores for the model constructs and then standardised the scores of the independent variable (legitimacy), the dependent variable (compliance), and the moderator (probability of a security incident) (Gaskin, 2020). We then created a new

TABLE 4 Correlations from the CFA.

Wave 1					
	MSUPPT_1	**INCON_1**	**ILLEGIT_1**	**COMPLI _1**	**PROB _1**
MSUPPT_1	**0.890**				
INCON_1	−0.114*	**0.884**			
LEGIT_1	−0.215***	0.628***	**0.773**		
COMPLI_1	0.297***	−0.291***	−0.427***	**0.815**	
PROB_1	0.055	0.017	0.010	0.013	**0.786**
Wave 2					
	MSUPPT_2	**INCON_2**	**ILLEGIT_2**	**COMPLI _2**	**PROB _2**
MSUPPT_2	**0.926**				
INCON_2	−0.136**	**0.905**			
LEGIT_2	−0.251***	0.658***	**0.788**		
COMPLI_2	0.302***	−0.361***	−0.439***	**0.842**	
PROB_2	0.020	0.097*	0.055	0.072	**0.770**
Wave 3					
	MSUPPT_3	**INCON_3**	**ILLEGIT_3**	**COMPLI _3**	**PROB _3**
MSUPPT_3	**0.922**				
INCON_3	−0.048	**0.904**			
LEGIT_3	−0.173***	0.611***	**0.778**		
COMPLI_3	0.323***	−0.283***	−0.435***	**0.839**	
PROB_3	0.008	0.110*	0.059	0.032	**0.813**

Note: $n = 529$. The numbers along the diagonal (in bold) are the square root of the AVE (average variance extracted); off-diagonal elements are correlations between constructs.
Abbreviation: CFA, confirmatory factor analysis.
*$p < 0.050$; **$p < 0.01$; ***$p < 0.001$.

TABLE 5 Goodness-of-fit statistics.

Wave	Model	CFI	SRMR	RMSEA	Hoelter's CN (0.01)
Wave 1	Measurement model	0.963	0.035	0.048	221
	Structural model	0.992	0.024	0.033	842
Wave 2	Measurement model	0.978	0.027	0.040	238
	Structural model	0.991	0.024	0.034	819
Wave 3	Measurement model	0.977	0.029	0.041	219
	Structural model	0.996	0.020	0.016	1168

Abbreviations: CFI, comparative fit index; RMSEA, root mean square error of approximation; SRMR, standardised root mean square residual.

interaction variable that represented the product of the independent variable and moderator. Next, we created a structural model and produced Johnson–Neyman plots in Amos (Gaskin & James, 2019) to assess the effect of the interaction on the relationship between the independent variable and the dependent variable. Johnson–Neyman plots are considered a highly accurate and rigorous method for evaluating interaction effects (Hayes & Matthes, 2009). The results of each of these tests are described below.

5 | RESULTS

Our analysis over the three waves fully supported three hypotheses (H1–H3), but did not support H4 (refer to Table 6 for details). Overall, these results provide important insights into the role of cybersecurity legitimacy in relation to employee compliance with cybersecurity policies. The total percentage of variance explained in wave 1 was 50.0% for cybersecurity legitimacy and 30.0% for compliance. During wave 2, total variance explained was 46.5% for legitimacy and 24.0% for compliance. Finally, in wave 3, total variance explained was 21.4% for legitimacy and 18.4% for compliance.

The first two hypotheses considered the mediating relationship of negative cybersecurity legitimacy with top management support and compliance (H1) and cybersecurity inconvenience and compliance (H2), respectively. Our results empirically supported both H1 and H2. For H1, standardised indirect effects were found to be significant between management support and compliance during wave 1 ($\beta = 0.07$, $p < 0.001$), wave 2 ($\beta = 0.05$, $p < 0.001$), and wave 3 ($\beta = 0.04$, $p < 0.001$). Consistent with past literature (e.g., D'Arcy & Greene, 2014; Humaidi & Balakrishnan, 2018), management support was also found to have a significant, direct relationship with cybersecurity policy compliance (refer to Table 7 for details) across all three waves. Using the classifications proposed by Zhao et al. (2010), the top management support——legitimacy——compliance relationship qualifies as a complementary mediation. For H2, standardised indirect effects were significant between cybersecurity inconvenience and compliance during wave 1 ($\beta = -0.31$, $p < 0.001$), wave 2 ($\beta = -0.18$, $p < 0.01$), and wave 3 ($\beta = -0.08$, $p < 0.001$). In comparison, the direct effects of inconvenience on compliance (refer to Table 7) were not significant across all three waves. Using the classifications proposed by Zhao et al. (2010), the inconvenience——legitimacy——compliance relationship qualifies as an indirect-only mediation.

For H3, negative cybersecurity legitimacy was found to be significantly and positively related to policy compliance during wave 1 ($\beta = -0.45$, $p < 0.001$), wave 2 ($\beta = -0.28$, $p < 0.001$), and wave 3 ($\beta = -0.19$, $p < 0.001$). As a result, H3 is supported.

In regard to H4, we find inconsistent evidence regarding the extent that the increased probability of a security incident dampens the negative relationship between negative cybersecurity legitimacy and compliance.

TABLE 6 Summary of results and hypotheses from the structural model.

Hypotheses		Beta and *p* values	Supported?
H1	Negative cybersecurity legitimacy mediates the positive relationship between top management support and cybersecurity policy compliance.	Wave 1: *Standardised indirect effects*: 0.07; $p < 0.001$ Wave 2: *Standardised indirect effects*: 0.05; $p < 0.001$ Wave 3: *Standardised indirect effects*: 0.04; $p < 0.001$	Yes
H2	Negative cybersecurity legitimacy mediates the negative relationship between cybersecurity inconvenience and cybersecurity policy compliance.	Wave 1: *Standardised indirect effects*: −0.31, $p < 0.001$ Wave 2: *Standardised indirect effects*: −0.18, $p < 0.01$ Wave 3: *Standardised indirect effects*: −0.08, $p < 0.001$	Yes
H3	Employees who judge cybersecurity activities to not be legitimate will comply less with cybersecurity policies.	*Standardised direct effects* Wave 1: −0.454, $p < 0.001$ Wave 2: −0.284, $p < 0.001$ Wave 3: −0.192, $p < 0.001$	Yes
H4	The probability of a cybersecurity incident dampens the negative relationship between negative cybersecurity legitimacy and cybersecurity policy compliance.	Wave 1: −0.077, *p* value 0.056 Wave 2: −0.069, *p* value 0.103 Wave 3: −0.027, *p* value 0.526	No

TABLE 7 Direct effects.

Relationship	Beta, *p* values
MSUPPT–LEGIT	Wave 1: $\beta = -0.139$, $p < 0.001$
	Wave 2: $\beta = -0.184$, $p < 0.001$
	Wave 3: $\beta = -0.207$, $p < 0.001$
MSUPPT–COMPLI	Wave 1: $\beta = 0.203$, $p < 0.001$
	Wave 2: $\beta = 0.244$, $p < 0.001$
	Wave 3: $\beta = 0.295$, $p < 0.001$
INCON–LEGIT	Wave 1: $\beta = 0.658$, $p < 0.001$
	Wave 2: $\beta = 0.620$, $p < 0.001$
	Wave 3: $\beta = 0.402$, $p < 0.001$
INCON–COMPLI	Wave 1: $\beta = 0.035$, NS
	Wave 2: $\beta = -0.074$, NS
	Wave 3: $\beta = -0.002$, NS

TABLE 8 Effects of control variables.

	Age	Gender	Education	Country	Income	Company size
LEGIT_1	0.04	0.05	0.00	−0.05	0.07*	0.04
LEGIT_2	0.00	−0.02	0.05	−0.02	0.04	0.02
LEGIT_3	0.02	−0.01	0.04	0.05	−0.01	−0.02
COMPLI_1	−0.04	0.01	0.01	−0.08*	−0.03	−0.09*
COMPLI_2	−0.04	0.07	0.00	−0.11**	0.00	−0.02
COMPLI_3	−0.12**	−0.03	−0.06	0.02	−0.04	−0.02

*$p < 0.05$; **$p < 0.01$.

During wave 1, the interaction between probability and legitimacy totalled −0.08 at $p = 0.056$; during wave 2, the interaction was −0.07 at $p = 0.103$; and during wave 3, the interaction was −0.027 at $p = 0.526$. Despite this marginal ($p < 0.10$) significance during wave 1, the non-significant results in waves 2 and 3 lead us to conclude that H4 is not supported. However, our Johnson–Neyman plot results suggest that moderation may still be present because the value of compliance does not equal zero for any values of legitimacy within the confidence intervals within the relevant range of values (Gaskin & James, 2019). In other words, these non-significant moderation effects may still be considered substantive based on the Johnson–Neyman criteria. Please refer to Appendix D for details.

We also examined the effects of six control variables (age, gender, education, country of residence, income, and number of company employees) on the two endogenous constructs (negative cybersecurity legitimacy and compliance). As noted in Table 8, age is negatively related to compliance (in wave 3 only), suggesting that older workers were less likely to comply with cybersecurity policies during October. Gender and education have no significant effect on either of the constructs in any of the three waves. Respondents who resided in the UK were less likely to comply with cybersecurity policies during wave 1 and wave 2, but were not significantly different from US respondents in wave 3. The income of participants was negatively related with negative cybersecurity legitimacy during wave 1, suggesting that employees who earn more are less likely to make negative legitimacy judgements, though this link did not hold in waves 2 and 3. Finally, company size was negatively related to compliance in wave 1, but this too did not hold during waves 2 and 3.

In summary, our results suggest that negative cybersecurity legitimacy does mediate the relationships between management support and policy compliance, as well as cybersecurity inconvenience and policy compliance. We also find empirical support for the significant negative link between negative cybersecurity legitimacy and policy compliance, but do not find clear support for the moderating role of the probability of a cybersecurity incident.

6 | DISCUSSION

Our results highlight several important insights regarding the cybersecurity behaviour of employees. First, we find that cybersecurity legitimacy is an important aspect of the policy compliance equation. It significantly mediates two constructs (management support and inconvenience) that have been hypothesised in past research to have either a direct relationship with compliance or be mediated by other constructs. Although we confirmed a significant direct relationship between management support and compliance in all three waves, none of our analysis supported a direct relationship between inconvenience and compliance. This result contrasts some past findings, including Hwang et al. (2017), but is consistent with other research noting a non-significant relationship, such as Ifinedo (2012). Regardless, the significant role of cybersecurity legitimacy is of importance, both as a mediator of organisational properties and behaviours, as well as having a direct relationship with policy compliance. Thus, we highlight a distinct view towards understanding why employees decide to comply with cybersecurity policies beyond the acknowledgement that 'management says we should' or 'it is inconvenient to follow the rules'. Rather, our findings lend validity to the perceptions-judgements-actions model of organisational legitimacy in a cybersecurity context. From a practice perspective, this result highlights the importance of managers not only undertaking cybersecurity initiatives, but also convincing employees that the organisation is acting in a legitimate manner. We view this as going beyond the standard training and awareness activities, which often highlight the general risks and threats posed by cybersecurity events. Although this is undoubtedly one element of demonstrating the legitimacy of cybersecurity initiatives to employees, our findings reinforce past research that argues for the importance of demonstrating that the organisation's response to these threats does not unnecessarily impact employees by restricting their autonomy, encroaching on their privacy, or threatening their work performance (e.g., Bijlsma-Frankema & Costa, 2010; Long et al., 2011). Further, our orientation on legitimacy expands past conceptualizations of cybersecurity fairness (e.g., Lowry et al., 2015), which focuses on harm caused to an employee's well-being and the attribution of blame (Folger & Cropanzano, 2001). Rather, by considering a broader range of employee norms, values, and beliefs, our results suggest that employees may not judge a cybersecurity initiative to be legitimate, even when their own well-being is not affected.

As our overarching contribution, we highlight the role of top management support and cybersecurity inconvenience in influencing compliance, via a mediated relationship with negative cybersecurity legitimacy. From a practical perspective, our results suggest that managers should be mindful not only of their organisation's cybersecurity behaviours and characteristics, but how these elements are perceived and judged by employees. In part, this view reinforces the sentiments of past research that advocate for education, training, and awareness (Bauer & Bernroider, 2017; Lowry et al., 2015), since such activities can help employees understand how to fulfil their cybersecurity responsibilities. However, our findings go beyond existing work by demonstrating the particular importance of convincing employees that cybersecurity initiatives are legitimate. That is, managers have a responsibility to not only design and implement appropriate cybersecurity initiatives, but also to ensure they are explained and sufficiently justified to employees in a manner that is consistent with their accepted norms and values. Although past research has employed theoretical lenses that consider related issues, our application of organisational legitimacy breaks new ground by extending the focus of employee judgements beyond only threats to well-being (i.e., fairness theory), but into broader considerations of the norms and values associated with cybersecurity initiatives.

Additionally, we examined the potential role of judgements of cybersecurity incident probability in moderating the link between legitimacy and behavioural compliance. Past research suggests that managers may seek to

periodically highlight the likelihood of a cybersecurity incident to employees as a means to elicit an awareness that will drive compliant behaviour (e.g., Johnston et al., 2015; Johnston & Warkentin, 2010). However, we did not find sufficient support for our hypothesis, which suggests that the legitimacy perceptions of employees are unyielding to differences in the risk characteristics of the cybersecurity incidents facing organisations. Practically, this finding is of concern for organisations because it suggests that if employees do not perceive cybersecurity initiatives to be legitimate, their corresponding level of policy compliance will remain unaffected, even if they are aware that an incident is highly likely to occur. In effect, our results suggest that the legitimacy judgements of employees outweigh their awareness of high probability incidents. For managers, this finding reinforces the preceding point suggesting the importance of convincing employees that cybersecurity initiatives are fair and reasonable, rather than relying on last-minute appeals to avoid particularly high-risk activities.

7 | LIMITATIONS AND FUTURE RESEARCH

We recognise several limitations of this study, which present promising opportunities for future research. First, we focus on two possible antecedents to legitimacy, but other antecedents are likely to exist and could be considered in future research, including cybersecurity training initiatives (e.g., D'Arcy et al., 2009; Lowry et al., 2015; Silic & Lowry, 2020) or cybersecurity policy quality (e.g., Goo et al., 2014; Pahnila et al., 2013). Both constructs represent organisational properties and behaviours that could be perceived by employees as an antecedent to employee legitimacy judgements, and employees may experience them to different extents over time (e.g., periodic cybersecurity training, changes in cybersecurity policies). Second, although we found insufficient support for the moderating role of judgements of cybersecurity incident probability, other constructs may help to more fully explain the judgement suppression phenomenon discussed by Bitektine and Haack (2015). For example, the rewards and sanctions levied by management regarding compliance behaviour could be considered as an additional moderator of the legitimacy to compliance relationship. Although past research finds that rewards and punishments have a relatively weak direct relationship with policy compliance (Cram et al., 2019), it may be that they take a more substantive role as a judgement suppressor (i.e., even when an employee judges a cybersecurity initiative to be illegitimate, they will still comply because of the promise of a reward or threat of a sanction). Third, our focus in this study was on the negative judgements of cybersecurity initiatives at a micro (i.e., individual employee) level. Future research could expand the spotlight to a wider range of legitimacy issues, including the focus on building positive legitimacy to enhance compliance, in contrast to attempts at decreasing negative legitimacy to avoid non-compliance. As well, future studies could investigate the broader, macro level legitimacy perceptions that are formed as stakeholders consolidate their views on an organisation's broader legitimacy status. Such studies could consider how these collective perceptions of an organisation's cybersecurity behaviour can impact company performance and drive organisational change (e.g., cybersecurity culture shifts). Although our study involves a multi-wave data collection, we stop short of explicitly theorising how particular events or behaviours can alter the perception-judgement-action process. In both the micro and macro cases, considering the role of time is likely to be an important factor in uncovering when and why change occurs. Finally, we acknowledge that the variance explained in our model declined with each successive wave, though it remains unclear why this occurred. It is possible that participants became habituated to the survey questions after each successive round and this influenced their responses. It is also possible that the explanatory power of the model was systematically influenced by factors associated with the ongoing COVID-19 pandemic, which we did not measure. Future research could attempt to further control for these factors by focusing on situations where the same organisational properties and behaviours are associated with different levels of legitimacy, such as collecting data from a range of employees within a single organisation. Considering the behaviour of both IT and non-IT employees may also be interesting in this context. Past research points out that individuals may differ in how they judge legitimacy depending on whether they place more value on flexibility or uncertainty avoidance (Bijlsma-Frankema & Costa, 2010). Such clarifications on the drivers of within-person aspects of cybersecurity

legitimacy would be another valuable theoretical contribution in future research, as well as providing practical insights to managers who seek to cultivate improved legitimacy in particular subsets of their employee population.

8 | CONCLUSION

This study sought to examine the role of cybersecurity legitimacy judgements by employees and the behavioural consequences of those judgements. Building on theory from the organisational legitimacy and the cybersecurity policy compliance literature, we conducted a three-wave study over 7 months with 529 participants. Our findings point to the important role of cybersecurity legitimacy in mediating the relationships between management support and policy compliance, as well as cybersecurity inconvenience and policy compliance. In doing so, we highlight promising new opportunities for future research on cybersecurity legitimacy and provide an impetus for research that delves into specific sources of variability regarding cybersecurity legitimacy and its behavioural outcomes.

DATA AVAILABILITY STATEMENT

Data available on request due to privacy/ethical restrictions.

ORCID

W. Alec Cram https://orcid.org/0000-0002-5819-3074
John D'Arcy https://orcid.org/0000-0003-0286-5772

REFERENCES

Addas, S., & Pinsonneault, A. (2018). E-mail interruptions and individual performance: Is there a silver lining? *MIS Quarterly*, *42*(2), 381–405.

Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extrarole performance. *Journal of Applied Psychology*, *91*(1), 221–232.

Ashforth, B. E., & Gibbs, B. W. (1990). The double-edge of organizational legitimation. *Organization Science*, *1*(2), 177–194.

Bagozzi, R. P., Yi, Y., & Phillips, L. W. (1991). Assessing construct validity in organizational research. *Administrative Science Quarterly*, *36*(3), 421–458.

Balozian, P., Leidner, D., & Warkentin, M. (2019). Managers' and employees' differing responses to security approaches. *Journal of Computer Information Systems*, *59*(3), 197–210.

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.

Bentler, P. M. (1992). On the fit of models to covariances and methodology to the Bulletin. *Psychological Bulletin*, *112*, 400–404.

Besnard, D., & Arief, B. (2004). Computer security impaired by legitimate users. *Computers & Security*, *23*, 253–264.

Bijlsma-Frankema, K. M., & Costa, A. C. (2010). Consequences and antecedents of managerial and employee legitimacy interpretations of control: A natural open system approach. In S. B. Sitkin, L. B. Cardinal, & K. M. Bijlsma-Frankema (Eds.), *Organizational control* (pp. 396–433). Cambridge University Press.

Bitektine, A., & Haack, P. (2015). The "macro" and the "micro" of legitimacy: Toward a multilevel theory of the legitimacy process. *Academy of Management Review*, *40*(1), 49–75.

Blunch, N. J. (2013). *Introduction to structural equation modeling using SPSS statistics and Amos* (2nd ed.). Sage.

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.

Cameron, A.-F., & Webster, J. (2013). Multicommunicating: Juggling multiple conversations in the workplace. *Information Systems Research*, *24*(2), 352–371.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of information security in the workplace: Linking information security climate to compliant behavior. *Journal of Information Privacy & Security*, *1*(3), 18–41.

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

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.

D'Arcy, J., & Greene, G. (2014). Security culture and the employment relationship as drivers of employees' security compliance. *Information Management & Computer Security*, *22*(5), 474–489.

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

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

Deephouse, D. L., & Suchman, M. (2008). Legitimacy in organizational institutionalism. In R. Greenwood, C. Oliver, K. Sahlin, & R. Suddaby (Eds.), *The SAGE handbook of organizational institutionalism* (pp. 49–77). SAGE Publications.

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.

Folger, R., & Cropanzano, R. (2001). Fairness theory: Justice as accountability. In J. Greenberg & R. Cropanzano (Eds.), *Advances in organizational justice* (pp. 1–55). Stanford University Press.

Fornell, C., & Larcker, D. F. (1981). Evaluating structural equation models with unobservable variables and measurement error. *Journal of Marketing Research*, *18*(1), 39–50.

Franke, G., & Sarstedt, M. (2019). Heuristics versus statistics in discriminant validity testing: A comparison of four procedures. *Internet Research*, *29*(3), 430–447.

Gaskin, J. (2020). *Structural equation modeling*. MyEducator.

Gaskin, J., & James, M. (2019). Johnson-Neyman plot analysis plugin for AMOS: Gaskination's StatWiki.

Gefen, D. (2000). E-commerce: The role of familiarity and trust. *Omega*, *28*, 725–737.

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.

Goodman, J. S., & Blum, T. C. (1996). Assessing the non-random sampling effects of subject attrition in longitudinal research. *Journal of Management*, *22*(4), 627–652.

Hair, J. F., Matthews, L. M., Matthews, R. L., & Sarstedt, M. (2017). PLS-SEM or CB-SEM: Updated guidelines on which method to use. *International Journal of Multivariate Data Analysis*, *1*(2), 107–123.

Hayes, A. F., & Matthes, J. (2009). Computational procedures for probing interactions in OLS and logistic regression: SPSS and SAS implementations. *Behavior Research Methods*, *41*(3), 924–936.

Henseler, J., Ringle, C. M., & Sarstedt, M. (2015). A new criterion for assessing discriminant validity in variance-based structural equation modeling. *Journal of the Academy of Marketing Science*, *43*(1), 115–135.

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.

Hoefer, R. L., & Green, S. E., Jr. (2016). A rhetorical model of institutional decision making: The role of rhetoric in the formation and change of legitimacy judgements. *Academy of Management Review*, *41*(1), 130–150.

Hoelter, J. W. (1983). The analysis of covariance structures: Goodness-of-fit indices. *Sociological Methods & Research*, *11*, 325–344.

Hsu, J. S.-C., Lee, J.-N., Fang, Y., Straub, D. W., & Ryu, H.-S. (2022). The role of vendor legitimacy in IT outsourcing performance: Theory and evidence. *Information Systems Research*, *33*(1), 337–361.

Hu, L. T., & Bentler, P. M. (1999). Cutoff criteria for fit indexes in covariance structure analysis: Conventional criteria versus new alternatives. *Structural Equation Modeling: A Multidisciplinary Journal*, *6*(1), 1–55.

Hu, Q., Dinev, T., Hart, P., & Cooke, D. (2012). Managing employee compliance with information security policies: The critical role of top management and organizational culture. *Decision Sciences*, *43*(4), 615–659.

Humaidi, N., & Balakrishnan, V. (2018). Indirect effect of management support on users' compliance behaviour towards information security policies. *Health Information Management Journal*, *47*(1), 17–27.

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.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security*, *31*(1), 83–95.

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

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

Johnston, A. C., Warkentin, M., Dennis, A. R., & Siponen, M. (2019). Speak their language: Designing effective messages to improve employees' information security decision making. *Decision Sciences*, *50*(2), 245–284.

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

Kahneman, D., & Tversky, A. (1979). Prospect theory: An analysis of decision under risk. *Econometrica*, *47*(2), 263–292.

Karahanna, E., Xu, S. X., Xu, Y., & Zhang, N. (2018). The needs-affordances-features perspective for the use of social media. *MIS Quarterly*, *42*(3), 737–756.

Karjalainen, M., Sarker, S., & Siponen, M. (2019). Toward a theory of information systems security behaviors of organizational employees: A dialectical process perspective. *Information Systems Research*, *30*(2), 687–704.

Kinnunen, S. (2016). *Exploring determinants of different information security behaviors*. (Master of Information Systems). University of Jyväskylä.

Kline, R. B. (2016). *Principles and practice of structural equation modeling* (4th ed.). The Guilford Press.

Kock, N. (2015). Common method bias in PLS-SEM: A full collinearity assessment approach. *International Journal of e-Collaboration*, *11*(4), 1–10.

Kothe, E. J., & Ling, M. (2019). Retention of participants recruited to a one-year longitudinal study via Prolific. *PsyArXiv*, 1–8. https://doi.org/10.31234/osf.io/5yv2u

Kraatz, M. S., & Zajac, E. J. (1996). Exploring the limits of the new institutionalism: The causes and consequences of illegitimate organizational change. *American Sociological Review*, *61*(5), 812–836.

Kuran, T. (1987). Preference falsification, policy continuity and collective conservatism. *The Economic Journal*, *97*(387), 642–665.

Kuran, T. (1995). *Private truths, public lies: The social consequences of preference falsification*. Harvard University Press.

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

Liang, H., Saraf, H., Hu, Q., & Xue, Y. (2007). Assimilation of enterprise systems: The effect of institutional pressures and the mediating role of top management. *MIS Quarterly*, *31*(1), 59–87.

Lindell, M. K., & Whitney, D. J. (2001). Accounting for common method variance in cross-sectional research designs. *Journal of Applied Psychology*, *86*(1), 114–121.

Long, C. P., Bendersky, C., & Morrill, C. (2011). Fairness monitoring: Linking managerial controls and fairness judgements in organizations. *Academy of Management Journal*, *54*(5), 1045–1068.

Lowry, P. B., & Moody, G. D. (2015). Proposing the control-reactance compliance model (CRCM) to explain opposing motivations to comply with organisational information security policies. *Information Systems Journal*, *25*(5), 465–488.

Lowry, P. B., Posey, C., Bennett, R. 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), 193–230.

Marsh, H. W., Hau, K.-T., & Wen, Z. (2004). In search of the golden rules: Comment on the hypothesis-testing approaches to setting cutoff values for fit indexes and dangers in overgeneralizing Hu and Bender's (1999) findings. *Structured Equation Modeling*, *11*(3), 320–341.

Menard, P., Bott, G. J., & Crossler, R. E. (2017). User motivations in protecting information security: Protection motivation theory versus self-determination theory. *Journal of Management Information Systems*, *34*(4), 1203–1230.

Meyer, J. W., & Rowan, B. (1977). Institutional organizations: Formal structure as a myth and ceremony. *American Journal of Sociology*, *83*(2), 340–363.

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

Narayanaswamy, R., Grover, V., & Henry, R. M. (2013). The impact of influence tactics in information system development projects: A control-loss perspective. *Journal of Management Information Systems*, *30*(1), 191–225.

Nunnally, J. C., & Bernstein, I. H. (1994). The assessment of reliability. In *Psychometric theory* (pp. 248–292). McGraw-Hill.

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.

Pahnila, S., Karjalainen, M., & Siponen, M. (2013). *Information security behavior: Towards multi-stage models* [Conference presentation]. Pacific Asia Conference on Information Systems, Jeju Island, South Korea.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). *Employees' behavior towards IS security policy compliance* [Conference presentation]. Proceedings of the 40th Hawaii International Conference on System Sciences, Waikoloa, HI.

Palan, S., & Schitter, C. (2018). Prolific.ac—A subject pool for online experiments. *Journal of Behavioral and Experimental Finance*, *17*, 22–27.

Pavlou, P. A., Liang, H., & Xue, Y. (2007). Understanding and mitigating uncertainty in online exchange relationships: A principal–agent perspective. *MIS Quarterly*, *31*(1), 105–136.

Peer, E., Brandimarte, L., Samat, S., & Acquisti, A. (2017). Beyond the Turk: Alternative platforms for crowdsourcing behavioral research. *Journal of Experimental Social Psychology*, *70*, 153–163.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method bias in behavioral research: A critical review of the literature and recommended remedies. *Journal of Applied Psychology*, *88*(5), 879–903.

Ponemon Institute. (2020). Cost of a data breach report. Retrieved from https://www.ibm.com/security/data-breach

Rowmanow, D., Rai, A., & Keil, M. (2018). CPOE-enabled coordination: Appropriation for deep structure use and impacts on patient outcomes. *MIS Quarterly*, *42*(1), 189–212.

Sanders, W. G., & Tuschke, A. (2007). The adoption of institutionally contested organizational practices: The emergence of stock option pay in Germany. *Academy of Management Journal*, *50*(1), 33–56.

Schnedler, W., & Vadovic, R. (2011). Legitimacy of control. *Journal of Economics and Management Strategy*, *20*(4), 985–1009.

Schoorman, F. D., & Mayer, R. C. (2008). The value of common perspectives in self-reported appraisals. *Organizational Research Methods*, *11*(1), 148–159.

Schuetz, S. W., Lowry, P. B., Pienta, D. A., & Thatcher, J. B. (2020). Effectiveness of abstract verus concrete fear appeals in information security. *Journal of Management Information Systems*, *37*(3), 723–757.

Scott, W. R. (1987). The adolescence of institutional theory. *Administrative Science Quarterly*, *32*(4), 493–511.

Semmer, N. K., Tschan, F., Meier, L. L., Facchin, S., & Jacobshagen, N. (2010). Illegitimate tasks and counterproductive work behavior. *Applied Psychology*, *59*(1), 70–96.

Shao, Z., & Li, X. (2022). The influences of three task characteristics on innovative use of malleable IT: An extension of adaptive structuration theory for individuals. *Information & Management*, *59*(3), 1–13.

Shropshire, J., Warkentin, M., & Sharma, S. (2015). Personality, attitudes, and intentions: Predicting initial adoption of information security behavior. *Computers & Security*, *49*, 177–191.

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.

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

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571–610.

Suddaby, R., Bitektine, A., & Haack, P. (2017). Legitimacy. *Academy of Management Annals*, *11*(1), 451–478.

Suddaby, R., & Greenwood, R. (2005). Rhetorical strategies of legitimacy. *Administrative Science Quarterly*, *50*(1), 35–67.

Tost, L. P. (2011). An integrative model of legitimacy judgments. *Academy of Management Review*, *36*(4), 686–710.

Tyler, T. R., & Blader, S. L. (2005). Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. *Academy of Management Journal*, *48*(6), 1143–1158.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management*, *49*(3–4), 190–198.

Verizon. (2020). 2020 Data breach investigations report. Retrieved from https://enterprise.verizon.com/resources/reports/dbir/

Voorhees, C. M., Brady, M. K., Calantone, R., & Ramirez, E. (2016). Discriminant validity testing in marketing: An analysis, causes for concern, and proposed remedies. *Journal of the Academy of Marketing Science*, *44*(1), 119–134.

Willer, R., Kuwabara, K., & Macy, M. W. (2009). The false enforcement of unpopular norms. *American Journal of Sociology*, *115*(2), 451–490.

Williams, L. J., Hartman, N., & Cavazotte, F. (2010). Method variance and marker variables: A review and comprehensive CFA marker technique. *Organizational Research Methods*, *13*(3), 477–514.

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.

Zhao, X., Lynch, J. G., & Chen, Q. (2010). Reconsidering Baron and Kenny: Myths and truths about mediation analysis. *Journal of Consumer Research*, *37*(2), 197–206.

AUTHOR BIOGRAPHIES

W. Alec Cram is an associate professor in the School of Accounting and Finance, University of Waterloo, Canada. His research focuses on how information systems control initiatives can contribute to improving the performance of organisational processes, including cybersecurity and algorithmic management. Alec serves as associate editor at the *Information Systems Journal* and holds the J. Page R. Wadsworth junior chair in Accounting and Finance.

John D'Arcy is a professor of MIS at the Lerner College of Business and Economics, University of Delaware, Newark, Delaware. He is also the SWUFE-UD Joint Educational Institute (JEI) Research Fellow. John's research interests include information security and IT risk management. He received his PhD from the Fox School of Business, Temple University. He currently serves as a senior editor of *MIS Quarterly* and an associate editor at the *Journal of the Association for Information Systems*.

How to cite this article: Cram, W. A., & D'Arcy, J. (2023). 'What a waste of time': An examination of cybersecurity legitimacy. *Information Systems Journal*, *33*(6), 1396–1422. https://doi.org/10.1111/isj.12460

APPENDIX A

MEASUREMENT ITEMS

During wave 1, we directed survey respondents to focus on the cybersecurity activities they were involved with in the preceding month, by specifying the time period they should consider when answering (e.g., 'My involvement with cybersecurity initiatives in April…'). For each subsequent wave, we updated the month.

Construct	Items
Top management support (Hu et al., 2012)	(1) Senior managers of our organisation have articulated a clear vision about cybersecurity. (2) Senior managers of our organisation have formulated a clear strategy for achieving a high degree of cybersecurity. (3) Senior managers of our organisation have established clear goals and objectives for achieving a high degree of cybersecurity.
Cybersecurity inconvenience (Bulgurcu et al., 2010)	(1) My involvement with cybersecurity initiatives during April held me back from doing my actual work. (2) My involvement with cybersecurity initiatives in April slowed down my response time to my colleagues, customers, managers, etc. (3) During April, my involvement with cybersecurity initiatives hindered my productivity at work. (4) In April, my involvement with cybersecurity initiatives impeded my efficiency at work.
Negative cybersecurity legitimacy (Alge et al., 2006; Kinnunen, 2016; Semmer et al., 2010)	(1) During April, I wondered if my participation in cybersecurity initiatives needed to be done at all. (2) During April, I wondered if my participation in cybersecurity initiatives made sense at all. (3) In April, I wondered if my participation in cybersecurity initiatives needed to be done because some people simply demand it that way. (4) My participation in cybersecurity initiatives during April went too far and should not have been expected from me. (5) It was unfair that I needed to participate in cybersecurity initiatives during April. (6) During April, I felt that my organisation's cybersecurity initiatives were an invasion of privacy. (7) The way that my organisation undertakes cybersecurity initiatives made me feel uneasy during April. (8) During April, my independence was restricted by having to participate in cybersecurity initiatives.[a]
Cybersecurity policy compliance (D'Arcy & Lowry, 2019)	(1) During April, I complied with my organisation's cybersecurity rules and regulations. (2) In April, I protected information and technology resources according to the requirements of my organisation's cybersecurity policy. (3) During April, I carried out my responsibilities, as prescribed in my organisation's cybersecurity rules and regulations. (4) My supervisor would say that I complied with my organisation's cybersecurity rules and regulations during April. (5) During April, my supervisor would say I protected information and technology resources according to the requirements of my organisation's cybersecurity policy. (6) During April, my supervisor would say I carried out my responsibilities, as prescribed in my organisation's cybersecurity rules and regulations.
Probability of a security incident (Herath & Rao, 2009)	(1) How likely is it that a security violation at your organisation will cause a significant outage that will result in loss of productivity? (2) How likely is it that a security violation at your organisation will cause a significant outage to the Internet that results in financial losses to organisations? (3) How likely is it that your organisation will lose sensitive data due to a security violation?

[a] Deleted based on item-validation process; items were rated on 7-point Likert scales, using 'strongly disagree' and 'strongly agree' anchors.

APPENDIX B

DEMOGRAPHIC DETAILS ON PARTICIPANTS

Demographic	Characteristic	Participants (% of total)
Age	29 years or younger	139 (26%)
	30–39 years	209 (40%)
	40–49 years	112 (21%)
	50–59 years	61 (12%)
	60 years or older	8 (2%)
Gender	Female	324 (61%)
	Male	201 (38%)
	Transgender	2 (0.4%)
	Do not identify as female, male, or transgender	2 (0.4%)
Education	No degree	16 (3%)
	High school degree	96 (18%)
	Bachelor's degree	264 (50%)
	Master's degree	111 (21%)
	Doctoral degree	19 (4%)
	Other degree (e.g., occupational, trade)	23 (4%)
Country of residence	UK	478 (90%)
	USA	51 (10%)
Income	Less than $40 000	110 (21%)
	$40 000–$59 999	172 (33%)
	$60 000–$79 000	106 (20%)
	$80 000–$99 999	76 (14%)
	$100 000 or more	65 (12%)
Company size	Less than 100	122 (23%)
	100–500	97 (18%)
	501–1000	44 (8%)
	1001–5000	104 (20%)
	More than 5000	162 (31%)

APPENDIX C

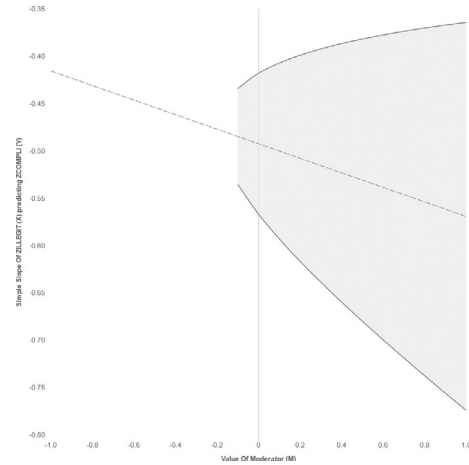
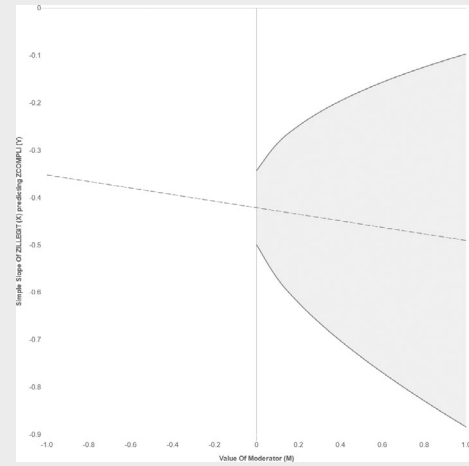
MEASUREMENT MODEL RESULTS

Construct	Items	Loadings	Cronbach's alpha
Wave 1			
MSUPPT_1	MSUPPT1_1	0.88	0.920
	MSUPPT2_1	0.83	
	MSUPPT3_1	0.96	
INCON_1	INCON1_1	0.90	0.935
	INCON2_1	0.85	
	INCON3_1	0.91	
	INCON4_1	0.88	
LEGIT_1	LEGIT1_1	0.78	0.912
	LEGIT2_1	0.81	
	LEGIT3_1	0.74	
	LEGIT4_1	0.79	
	LEGIT5_1	0.80	
	LEGIT6_1	0.75	
	LEGIT7_1	0.72	
COMPLI_1	COMPLI1_1	0.80	0.922
	COMPLI2_1	0.79	
	COMPLI3_1	0.78	
	COMPLI4_1	0.86	
	COMPLI5_1	0.82	
	COMPLI6_1	0.83	
PROB_1	PROB1_1	0.91	0.827
	PROB2_1	0.74	
	PROB3_1	0.69	
Wave 2			
MSUPPT_2	MSUPPT1_2	0.92	0.947
	MSUPPT2_2	0.91	
	MSUPPT3_2	0.95	
INCON_2	INCON1_2	0.90	0.948
	INCON2_2	0.85	
	INCON3_2	0.94	
	INCON4_2	0.92	
LEGIT_2	LEGIT1_2	0.82	0.920
	LEGIT2_2	0.83	
	LEGIT3_2	0.71	
	LEGIT4_2	0.86	
	LEGIT5_2	0.77	
	LEGIT6_2	0.77	
	LEGIT7_2	0.75	

Construct	Items	Loadings	Cronbach's alpha
COMPLI_2	COMPLI1_2	0.77	0.936
	COMPLI2_2	0.84	
	COMPLI3_2	0.85	
	COMPLI4_2	0.87	
	COMPLI5_2	0.84	
	COMPLI6_2	0.88	
PROB_2	PROB1_2	0.91	0.810
	PROB2_2	0.75	
	PROB3_2	0.62	
Wave 3			
MSUPPT_3	MSUPPT1_3	0.96	0.945
	MSUPPT2_3	0.88	
	MSUPPT3_3	0.92	
INCON_3	INCON1_3	0.90	0.947
	INCON2_3	0.88	
	INCON3_3	0.93	
	INCON4_3	0.91	
LEGIT_3	LEGIT1_3	0.84	0.915
	LEGIT2_3	0.81	
	LEGIT3_3	0.78	
	LEGIT4_3	0.80	
	LEGIT5_3	0.78	
	LEGIT6_3	0.70	
	LEGIT7_3	0.73	
COMPLI_3	COMPLI1_3	0.76	0.934
	COMPLI2_3	0.79	
	COMPLI3_3	0.87	
	COMPLI4_3	0.88	
	COMPLI5_3	0.83	
	COMPLI6_3	0.89	
PROB_3	PROB1_3	0.88	0.854
	PROB2_3	0.82	
	PROB3_3	0.73	

APPENDIX D

INTERACTION RESULTS

Interaction	Estimate	*p* Value	Johnson–Neyman plot
Wave 1: Legitimacy × Probability → Compliance	−0.077	0.056	
Wave 2: Legitimacy × Probability → Compliance	−0.069	0.103	
Wave 3: Legitimacy × Probability → Compliance	−0.027	0.52