Information Systems Frontiers (2023) 25:1439–1458
https://doi.org/10.1007/s10796-022-10281-6

An Investigation of the Factors that Influence Job Performance During Extreme Events: The Role of Information Security Policies

Victoria Kisekka[1] · **Sanjay Goel**[2]

Accepted: 21 April 2022 / Published online: 1 June 2022

Abstract
Diligent compliance with Information security Policies (ISP) can effectively deter threats but can also adversely impact organizational productivity, impeding organizational task completion during extreme events. This paper examines employees' job performance during extreme events. We use the conservation of resources (COR) theory to examine how psychological resources (individual resilience, job meaningfulness, self-efficacy) and organizational resources (incident command leadership, information availability, and perceived effectiveness of security and privacy controls) influence ISP compliance decisions and job performance during extreme events. The results show that a one-size-fits-all approach to ISP is not ideal during extreme events; ISP can distract employees from critical job tasks. We also observed that under certain conditions, psychological resources, such as individual resilience, are reserved for job performance, while others, such as self-efficacy, are reserved for ISP compliance. A post hoc analysis of data from respondents who experienced strain during a real extreme event while at work was conducted. Our discussion provides recommendations on how security and privacy policies can be designed to reflect disaster conditions by relaxing some policy provisions.

Keywords Job performance, Security policy compliance · Extreme events · Security behavior

1 Introduction

A good information security management program must have a strategy for dealing with unplanned extreme events (Baskerville et al., 2014). An extreme event is a sudden unplanned incident resulting in severe disruption of normal operations and continuity of services. These events can be environmental (floods, earthquakes, fires, etc.), societal (mass shootings, terrorist attacks, etc.), or organizational (e.g., financial losses, disrupted supply line, etc.). The current literature mostly focuses on prevention strategies for adverse events, which by themselves do not successfully deal with managing security and privacy during extreme events. Of critical importance to organizations operating during extreme events is creating a set of security guidelines that incorporate not only aspects of prevention but also adaptive capacity and readiness to counter unforeseeable security threats (Baskerville et al., 2014, p. 140). The need to balance ISP compliance and performance has created tension between security and privacy on the one hand, and utility on the other. For example, people often weigh their privacy against other tangible benefits, such as fame, convenience, material gain, and access to information (Rainie & Duggan, 2016). In organizations, however, adherence to privacy regulations is typically sacrosanct, with little room for flexibility, due to focus of regulatory compliance. By creating rigid ISP, are organizations hindering employee job performance during extreme events? For instance, in the event of a mass shooting, would it be more important for a hospital to secure information resources and protect patient privacy or to save people from dying? In an extreme event situation, should employees be empowered to focus solely on their non-security-related job tasks and on managing the extreme event,

✉ Sanjay Goel
goel@albany.edu

Victoria Kisekka
vkisekka@albany.edu

[1] Information Security and Digital Forensics, School of Business, Massry Center for Business (BB) 371, University at Albany, State University of New York, 1400 Washington Ave., Albany, NY 12222, USA

[2] Information Security and Digital Forensics, School of Business, Massry Center for Business (BB) 311, University at Albany, State University of New York, 1400 Washington Ave., Albany, NY 12222, USA

without the added mental stress of possible ISP compliance violations? This research sought to answer these questions by examining the compliance versus utility dilemma during extreme events. The specific questions that guided this research are as follows: (1) What factors influence employee ISP compliance intentions during extreme events? (2) How do ISP compliance intentions influence perceived job performance during extreme events?

There has been a lot of work on using deterrence theory and protection motivation theory (Trang & Brendel, 2019) and the impact of training (Kweon et al., 2021) and awareness (Kam et al., 2020) in improving ISP compliance. Yang and Lee (2016) specifically use protection motivation theory on healthcare workers and suggest that awareness of cyber security threats and satisfaction with security technicity and policies improve ISP compliance. We argue that despite security and privacy awareness training, employees may choose to ignore privacy and security needs over job performance during an extreme event. As a result, different interventions are still needed to improve ISP compliance and overall job performance during extreme events when the demands on cognitive capacity of employees is high.

The issue of information security and privacy versus utility has been studied extensively in the computer science literature, in which techniques for obfuscation and aggregation have been used to anonymize data, often at the cost of data utility (Barth et al., 2007; Chakraborty et al., 2013; Halperin et al., 2008; Sankar et al., 2013; Wu et al., 2013). The right balance between information security and privacy, and utility is often context-driven and requires understanding how people make conscious choices to achieve something of societal value (such as national security, public health, and economic efficiency) (Tene & Polonetsky, 2012; Goel, 2015). Research on information security and privacy versus utility in the information systems literature is scarce.

We examined the information security and privacy versus utility dilemma in human reasoning by assessing how employees operate under strain during extreme events. In particular, we identified contextual factors that drive employees' decisions related to ISP compliance and job performance during extreme events. We used the lens of conservation of resources (COR) theory (Hobfoll, 1989) to study how employees utilize psychological and organizational resources to balance the demands of ISP compliance with urgent work tasks to maintain high levels of job performance during extreme events. Survey data were used to test the hypothesized model; respondents were given a scenario for an extreme event and asked to role play. A post hoc study was conducted as well. Here, we sought to test our research model with a population sample of individuals who had experienced a real extreme event while at work.

The rest of the paper is organized as follows: Sect. 2 provides an overview of the literature; Sect. 3 provides the theoretical model and hypotheses; Sect. 4 provides our methods; Sect. 5 provides a discussion with recommendations for harmonizing ISP to ground realities by creating policies that balance information security and utility; lastly, Sect. 6 provides some concluding remarks.

2 Literature Review

2.1 Employee Job Performance During Extreme Events

There are consistent findings on the negative impact of employee strain on work performance during extreme events. Organizational behavior, occupational health, and other related disciplines have long established that extreme events in the workplace severely degrade the continuity of operations due to several factors, including stress, decreased performance, and resource shortages (Arshadi & Damiri, 2013). At the same time, researchers and analysts together with government agencies charged with emergency management efforts have developed emergency response and recovery methodologies (Federal Emergency Management Agency 2010; Federal Emergency Management Agency 2019; Roberts, 2006; Scarinci, 2014). Federal Emergency Management Agency (FEMA) methodologies have been widely adopted in the IS literature in different contexts, such as managing emergencies related to information technology (IT) incidents (Järveläinen, 2013), security incidents (Baskerville et al., 2014; Mitropoulos et al., 2006), and cloud computing incidents (Ab Rahman & Choo, 2015). Despite these efforts, emergency response and recovery plans tend to be conceptual, with insufficient details, and do not typically address IT risks that may seem insignificant yet carry great risk of decreased employee productivity (Ab Rahman & Choo, 2015; Hiller et al., 2015; Hove et al., 2014; Scarinci, 2014). Research efforts that *have* addressed IT tend to place greater emphasis on technical details than on policies and standards (Ahmad et al., 2012).

Related research evidence suggests that several challenges still prevent the attainment of optimal information security during emergency responses. Observations of previous events indicate that in some instances, employees had the competence to respond, but a lack of communication and coordination caused inefficiencies in managing response activities (Ab Rahman & Choo, 2015; Abramson & Redlener, 2012; Ahmad et al., 2012, 2015; Bharosa et al., 2010; Hove et al., 2014; Tøndel et al., 2014). In other instances, employees lacked the ability to conduct timely vulnerability assessments and real-time monitoring of potential security risks (Ahmad et al., 2012). Elsewhere, inefficiencies stemmed from a failure to involve employees in emergency planning activities, which resulted in confusion, a lack of

understanding of responsibilities, and even unintended non-compliance with ISP (Ahmad et al., 2015; Hove et al., 2014; Tøndel et al., 2014). Scholars have also attributed failures to the lack of management support during turbulence (Devitt & Borodzicz, 2008; Morrison et al., 2014). For instance, Morrison et al. (2014) reported that while senior managers participate in emergency planning, their participation during actual emergencies is often lacking, with no chain of command available to manage activities. This research provides a good understanding of the role of organizational resources in achieving high job performance; however, the potential role of personal resources when employees are under strain during extreme events has received minimal attention. Moreover, our knowledge of the factors that influence job performance when employees are charged with other responsibilities, such as ISP compliance, is still limited. Our research addresses these limitations.

2.2 Information Security Policy (ISP) Compliance

The information security (IS) literature has determined that ISP compliance decisions are influenced by both positive and negative reinforcements (Chen et al., 2012; Pahnila et al., 2007). Positive reinforcements are factors that motivate compliant behavior. When a positive reinforcement is introduced to an employee's work environment, it results in favorable attitudes about security policies, subsequently increasing the likelihood of ISP compliance. On the other hand, negative reinforcements motivate compliant behavior by removing an unfavorable stimulus from the employee's work environment. Here, the literature has established that unfavorable factors, such as punishments, induce fear and discourage non-compliant behavior (Johnston & Warkentin, 2010). In other words, compliance stems from the fear of the cost of non-compliance, which could take many different forms, such as punishments, a poor performance evaluation score, denial of a salary raise, or possible job termination. Theoretically, this phenomenon has previously been explained by rational-based theories. The extant literature explains that ISP compliance decisions follow a rational decision-making process whereby employees evaluate the consequences of non-compliance against the benefits of compliance (Bulgurcu et al., 2010; Pahnila et al., 2007). Accordingly, beliefs about the relative benefits of compliance and non-compliance shape employees' attitudes about ISP compliance.

A closely related theory used to describe ISP compliance is the theory of planned behavior (TPB) (Ajzen, 1985, 1991). TPB posits that ISP compliance intentions are preceded by attitudes toward security policies, normative beliefs, and self-efficacy with regard to completing compliance tasks. Several positive and negative reinforcements have been shown to strengthen the three determinants of ISP compliance intentions. These include organizational and personal factors. Organizational factors relate to resources that the organization provides to strengthen ISP compliance intentions by modifying attitudes, reinforcing social norms, and boosting self-efficacy. Numerous organizational factors have been identified in the literature, including leadership, security training, and security communication resources (Chan et al., 2005; Herath & Rao, 2009b; Hu et al., 2012; Puhakainen & Siponen, 2010). Another commonly studied category of organizational factors that influence ISP compliance intentions are technical resources, which include automated security controls, and communication and collaboration capabilities (Safa et al., 2016). Contrary to organizational factors, there are personal factors such as those relating to cognitive beliefs, including trust, intrinsic psychological motivators (e.g., self-determination, perceived autonomy, self-efficacy), and perceived support, which influence ISP compliance (Herath & Rao, 2009a; Ifinedo, 2014; Vance et al., 2012; Wall et al., 2013). Protection motivation theory (PMT) has also been widely applied to understand ISP compliance, either alone or in combination with the theories discussed above (Herath & Rao, 2009b). PMT describes the cognitive processes that govern an individual's decision to protect an organization's assets from security threats (Herath & Rao, 2009b; Ifinedo, 2012; Johnston & Warkentin, 2010; Pahnila et al., 2007; Siponen et al., 2014; Vance et al., 2012). Research findings suggest that this process involves two types of appraisals: a threat appraisal, which focuses on the perceived severity of the threat and the vulnerability of the organization's assets to that threat; and a coping appraisal, which focuses on preventative behavior (such as self-efficacy and response efficacy) to mitigate the negative effects of the threat (Herath & Rao, 2009b; Johnston & Warkentin, 2010; Pahnila et al., 2007; Siponen et al., 2014; Vance et al., 2012; Wall et al., 2013).

An understudied topic in the literature is how contextual factors related to extreme events in the workplace influence employees' ISP compliance decisions. Turbulence in the workplace is inevitable, but an organization's ability to withstand the devastating impact of turbulence depends on how well the disaster response and recovery processes are managed. Past research provides a deep understanding of how individuals make ISP compliance decisions during normal working conditions; however, generalizing these findings to extreme events, characterized by chaos, stress, resource scarcity, and uncertainty can be misleading. This research addresses this limitation by identifying contextual factors that may affect ISP compliance intentions during conditions of an extreme event.

3 Theoretical Background

A theory that has been widely used to describe how individuals react to stressful events is COR theory (Hobfoll, 1989). COR theory posits that during stressful events, individuals actively seek to avoid loss by engaging in loss-countering strategies. When confronted with stressful working conditions that threaten resource availability, individuals will find ways to create new resources in an effort to counter the potential decline in performance effectiveness (Hobfoll, 1989, 2002; Maslach et al., 2001). Resources are defined as "any objects, personal characteristics, or conditions that serve as a means of attainment of objectives" (Hobfoll, 1989, p. 516). A threat to resource availability triggers a coping mechanism whereby individuals utilize their internal psychological resources, along with other external resources available to them to deal with strain. The COR theory has been applied mainly in the psychological literature; however, similar coping models have been introduced in the IS discipline. Pertinent examples include a two-stage coping model for adapting to IT threats (Beaudry, 2009; Beaudry & Pinsonneault, 2005). The first stage in the model is appraisal where the individual forms an opinion of the level of risk associated with the perceived threat. The second stage is adaptation, whereby the individual engages in threat-avoidance and benefit-maximizing behavior. The positive outcomes of successful adaptation include, but are not limited to, individual efficiency, performance effectiveness, and a reduction of negative consequences. Similarly, Liang and Xue (2009) proposed and validated a threat-avoidance model theorizing that following the appraisal of an IT threat, an individual will mitigate the threat by engaging in protective coping behaviors.

Implicit in these studies is the viewpoint that due to strain resulting from extreme events, an employee's psychological disposition can significantly attenuate the devastating effects of the strain on work efficiency. The change in psychological disposition denotes a primary coping process by which the employee identifies resources—both internal (psychological resources) and external (such as organizational resources)—to facilitate adaptation and the achievement of positive work outcomes.

We adopted the COR theory (Hobfoll, 1989) and the coping model (Beaudry & Pinsonneault, 2005) to demonstrate the critical role of psychological and organizational resources in motivating ISP compliance and individual performance during extreme events. We maintain that during stressful working conditions, employees rely on their own internal psychological resources, as well as on available organizational resources, to maintain work efficiency—specifically, continued compliance with ISP and individual performance effectiveness. Psychological resources that relate to coping and adapting to adversity have received little to no attention in the ISP compliance literature. We propose two new psychological resources that we contend are essential for adapting to strain in a work environment—namely, individual resilience and job meaningfulness. Individual resilience is defined as an individual's ability to cope and adapt to stressful situations (Smith et al., 2008). We define job meaningfulness as the degree to which one perceives their work to significantly impact others (such as colleagues and the organization as a whole) in a positive way (Rosso et al., 2010). A third variable that has been widely studied is self-efficacy. Acknowledging previous research on the important role of self-efficacy in motivating compliance decisions, we included it in our model as well. Consistent with COR theory and related IS research (e.g., (Liang & Xue, 2009), we also included three organizational factors in our model: incident command leadership, perceived effectiveness of security controls, and information availability. A detailed discussion of construct definitions and hypothesis development is provided in the following sections.

3.1 Hypothesis Development

Psychological Resources Psychologists have long established that during stressful events, individuals will rely on their psychological attributes as a defense mechanism to achieve positive outcomes for themselves, for their friends and peers, or for the organization as a whole (Erez & Judge, 2001). The extant literature in psychology and behavioral studies has linked internal resources of self-evaluation and self-motivation to goal commitment and positive performance outcomes (Erez & Judge, 2001; Karimi & Alipour, 2011; Ng et al., 2006). Individuals believe to a great extent that outcomes of events are contingent on internal (psychological) resources. Internal resources specifically, locus of control and self-efficacy determine how individuals react to disturbances in their environment and the extent to which individuals are motivated to control the outcomes in their environment (Erez & Judge, 2001). Individuals who exhibit high levels of locus of control and self-efficacy perceive themselves to have more control over their environment (Spector, 1982, p. 11). Additionally, individuals with high levels of internal resources have a high sense of self-drive, posess self-motivation to independently initiate tasks and take action, and cope faster when faced with uncertainties (Anderson, 1977; Spector, 1982). This study sought to focus on internal variables that motivate performance and positive job outcomes (such as task performance, and compliance) through self-evaluation (Erez & Judge, 2001; Spector, 1982). We therefore limited our study to three factors which are related to locus of control and are essential for managing and coping with stress during extreme events in an

organizational setting, namely, self-efficacy, job meaning, and resilience.

In a way, individuals who possess the psychological resources needed to deal with stressful events form a psychological contract with the organization and become profoundly invested in contributing to the organization's goals. IS scholars have also demonstrated that intrinsic motivators strengthen ISP compliance intentions (Herath & Rao, 2009a). Psychological resources, such as job meaningfulness and self-efficacy, have been linked to enhanced performance, work effectiveness, and work motivation (Morgeson et al., 2012). The process of protective behaviors is initiated when an individual perceives strain in the workplace as posing a threat. This is followed by inevitable psychological changes that assist with adaptation to the new, unstable environment. In this process of adaptation, individuals will shift their psychological state to states that are more suitable and appropriate for dealing with the stress caused by extreme events in their environment (Cascio, 2003; Morgeson et al., 2012). This will result in enhanced work effectiveness and work commitment, which can take the form of compliance (Cascio, 2003; Herath & Rao, 2009a; Morgeson et al., 2012). In this research, we focused on three psychological resources, namely, individual resilience, job meaningfulness, and self-efficacy, hypothesizing that each resource has a positive effect on ISP compliance during extreme events. The hypothesized research model is shown in Fig. 1.

Individual Resilience Resilience is a protective state that facilitates the ability to overcome adversity through coping and adaptation (Fletcher & Sarkar, 2013; Ong et al., 2006). The benefits of resilience have been well documented. For instance, psychologists have long shown that people who experience trauma during childhood are more likely to live happier and more fulfilling adult lives *if* they are highly resilient. Likewise, resilience plays a significant role in lowering the effects and likelihood of post-traumatic stress disorder among disaster victims (Fletcher & Sarkar, 2013). The organizational behavior literature has also demonstrated that resilient employees adapt very quickly to changes in the workplace with few complications. A resilient employee is likely to exhibit the mental strength needed to remain optimistic while also embracing setbacks associated with abrupt changes. We expect to make similar observations in the context of ISP compliance and job performance during disturbances in the workplace. Specifically, we expect that because ISP is instituted to ensure that computer resources are safely protected from adversaries; ISP compliance is one way through which this objective can be achieved. Compliance with ISP is an essential element of employee efficiency in terms of achieving the greater good of protecting resources from security risks, just as dedication is essential to effectively performing work tasks and successfully meeting work objectives. In the workplace, strain induced by extreme events of any magnitude threaten these objectives and thus provoke the mental state of resilience, which will in turn increase the likelihood of an employee engaging in desirable behavior, such as ISP compliance. Employees with a high level of individual resilience will be more likely to perform their job well and to possess stronger ISP compliance intentions compared to employees with a low level of individual resilience. Thus:

H1a: During extreme events, individual resilience will have a positive effect on ISP compliance intentions.
H1b: During extreme events, individual resilience will have a positive effect on perceived individual job performance.

Job Meaningfulness Meaningfulness refers to the degree of significance that an individual attaches to a given object (Rosso et al., 2010). A growing body of research suggests that job meaningfulness is one of the most important psychological traits needed to improve job performance (Cascio, 2003; Morgeson et al., 2012; Rosso et al., 2010).

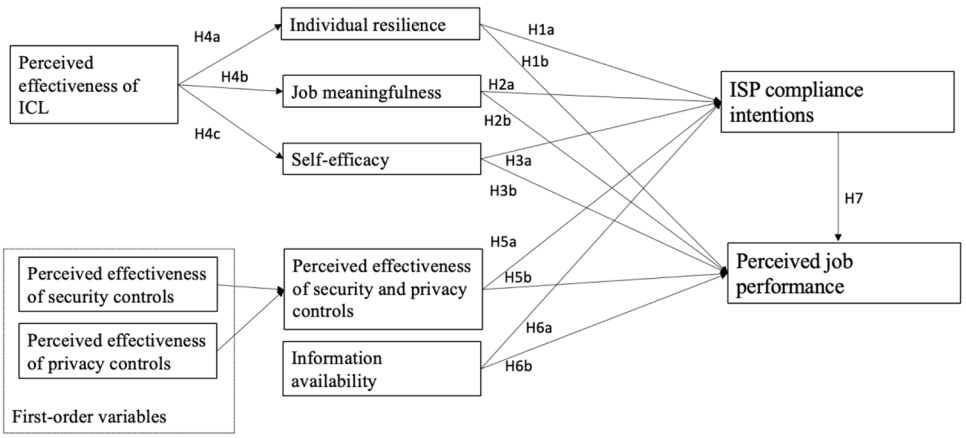

Fig. 1 Conceptual model of the factors that influence perceived job performance during extreme events

Meaningful work motivates individuals to engage in the constructive behaviors necessary for achieving performance goals. Employees who believe that their work benefits others will lend their efforts to achieving the greater good (Rosso et al., 2010). Similarly, employees who believe that their work is meaningful will engage in behaviors that contribute to the organization's overall goals; e.g., performing work tasks more efficiently to ensure the attainment of broader organizational objectives. Complying with the organization's policies constitutes one type of contribution to the achievement of performance goals related to security management. We suspect that when confronted with an unstable, chaotic work environment, employees who perceive their work to be meaningful would exhibit a greater level of engagement and involvement in performing tasks of benefit to the organization, such as complying with ISP. This is because non-compliance would expose the organization to greater risk of security attacks, which would represent the antithesis of meaningful and beneficial work. The relationship between meaning and positive performance outcomes has also been considered to be significant in the context of extreme events (Britt et al., 2001). Against this backdrop, we expect that during an extreme event, a sense of meaning in relation to work will shape employees' behavior by increasing their desire to perform their job well and protect information resources through compliance. Therefore, we hypothesized:

H2a: During extreme events, job meaningfulness will have a positive effect on ISP compliance intentions.
H2b: During extreme events, job meaningfulness will have a positive effect on perceived individual job performance.

Self-efficacy One of the most widely studied personal attributes in the IS literature is self-efficacy. Self-efficacy significantly motivates compliance intentions and performance effectiveness, as has been previously shown (Chan et al., 2005; Herath & Rao, 2009a; Siponen et al., 2014). Positive self-perceptions regarding one's ability to handle security challenges will bolster interest and desire to achieve security goals, such as conforming to established privacy and security regulations. We theorize that the relationship between self-efficacy and ISP compliance intentions, as well as between self-efficacy and job performance, when dealing with extreme events in the workplace will be similar. Further, employees who have strong beliefs in their ability to successfully execute security tasks and other assigned job duties will develop equally strong intentions for ISP compliance, as well as for completing work tasks and meeting performance goals. In judging themselves to possess the ability to work efficiently and effectively, these employees will form a sense of commitment to follow through with the achievement of performance goals. We therefore hypothesize:

H3a: During extreme events, self-efficacy will have a positive effect on ISP compliance intentions.
H3a: During extreme events, self-efficacy will have a positive effect on perceived individual job performance.

Organizational Resources Besides internal psychological resources, resources provided by the organization also drive ISP compliance decisions. This research focused on three organizational resources that are relevant to achieving positive outcomes during extreme events: perceived effectiveness of incident command leadership (ICL), perceived effectiveness of security and privacy controls, and information availability.

Incident Command Leadership (ICL) ICL refers to the command and control structure responsible for managing all aspects of a disturbance, including (but not limited to) role assignment, resource distribution, and the supervision of all activities related to the disturbance (Federal Emergency Management Agency 2018). Intrinsic factors alone may not be sufficient to motivate ISP compliance and performance effectiveness during extreme events. Some individuals will naturally possess adequate levels of resilience, job meaningfulness, and self-efficacy, while others may need assistance in strengthening these internal attributes. Notwithstanding the level of individual resilience, job meaningfulness, and self-efficacy, strain at work will require other tools to ensure optimal performance outcomes. Considerable research has shown that leadership indirectly promotes productive work behaviors through intrinsic motivation (Charbonneau et al., 2001; Hannah et al., 2016). When employees perceive their leaders to be supportive, they are more likely to exhibit greater self-efficacy and perceive their work to be more meaningful (Carton, 2018; Hannah et al., 2016). The relationship between leadership and positive psychological attributes is explained by the theory of transformational leadership, which posits that positive perceptions about a leader elicit positive responses (Lowe, Galen Kroeck, & Sivasubramaniam, 1996). We propose that an employee's perception of how well leaders are managing operations during extreme events will have a positive influence on the employee's level of individual resilience, job meaningfulness, and self-efficacy. Employees who believe that their leader is supporting work efforts and activities during extreme events may feel inspired to respond positively to associated changes in the environment. For example, leadership that instills hope in employees may engender feelings of resilience, prompting employees to no longer perceive the turbulence to be overwhelming and unmanageable. Job

meaningfulness can be cultivated by leaders who support their subordinates in creating a greater connection between work tasks and the organization's goals. Support in the form of providing information related to how ISP compliance and work efficiency during extreme events contribute to the organization's security and performance objectives, respectively, may increase employees' sense of connectedness to the organization. Such connectedness generates a sense of meaning in the employees' work. In regard to self-efficacy, we predict that because leadership and self-efficacy have a significant positive relationship (Hannah et al., 2016), a similar link would be observed during extreme events. We theorize that employee perceptions of how well the leadership team is managing extreme events (e.g., addressing emerging problems, guiding employees, strategically managing security risks, efficiently allocating resources) will foster a greater sense of competence in security and work tasks. As such, we hypothesize:

H4a: During extreme events, the perceived effectiveness of ICL will have a positive effect on individual resilience.
H4b: During extreme events, the perceived effectiveness of ICL will have a positive effect on job meaningfulness.
H4c: During extreme events, the perceived effectiveness of ICL will have a positive effect on self-efficacy.

Perceived Effectiveness of Security and Privacy Controls This variable pertains to an employee's judgement of how well the organization's security and privacy controls are protecting resources from security and privacy threats. Effective controls contribute to the organization's security objectives by allowing resources to successfully operate as expected for example, by accurately detecting and blocking unauthorized access to computer networks or by verifying the credentials of authorized users accurately and in a timely manner. During normal working conditions, an individual's perceived effectiveness in his or her ability to perform security tasks significantly strengthens ISP compliance intentions (Herath & Rao, 2009a). The importance of perceived security is underscored in the occupational health literature, where scholars have empirically demonstrated that feelings of safety lead to a significant increase in employee productivity and engagement in work tasks (Whiteoak & Mohamed, 2016). Also, employees' compliance to safety requirements is motivated by perceptions of a safe work environment (Clarke, 2006). Similarly, we postulate that perceptions related to the effectiveness of security and privacy controls will result in a higher likelihood of ISP compliance intentions and the successful completion of work tasks. In a way, the belief that security and privacy controls are working as expected reinforces the importance of security to the organization. This further strengthens an employee's desire to contribute to the organization's security and performance objectives through ISP compliance and work productivity. Thus, we hypothesize:

H5a: During extreme events, the perceived effectiveness of security and privacy controls will have a positive effect on ISP compliance intentions.
H5b: During extreme events, the perceived effectiveness of security and privacy controls will have a positive effect on perceived individual job performance.

Information Availability The availability of information is of great importance to achieving desirable outcomes when the organization is operating during extreme events. All aspects of information security—confidentiality, integrity, availability—are essential for disaster response management; however, evidence suggests that responders are more concerned with availability (Bharosa et al., 2010). Past literature suggests that factors related to information access result in positive outcomes, such as policy compliance (Bauer et al., 2017). We make similar predictions that the availability of critical information to employees under strain (induced by extreme events) will enhance the likelihood of ISP compliance intentions and performance effectiveness. This leads us to hypothesize:

H6a: During extreme events, information access will have a positive effect on ISP compliance intentions.
H6b: During extreme events, information access will have a positive effect on perceived individual job performance.

ISP Compliance Intensions Employees are expected to not only comply with ISP during extreme events but also complete work tasks efficiently. The demands of complying with ISP coupled with fatigue and exhaustion increase an employee's workload during an extreme event, consequently lowering employees' ability to perform job tasks effectively. A strict information security and privacy regimen implemented through access control rules and ISP can effectively deter threats and manage privacy mandates; however, it can also adversely impact organizational productivity and impede the completion of organizational tasks when operating during extreme events. This is because ISP impose limitations on employees, hindering them from performing other tasks, especially during a time when agility and speed can be critical. Thus, we hypothesize as follows:

H7: During extreme events, ISP compliance will have a negative effect on perceived individual job performance.

4 Research Methodology

4.1 Data Collection Procedure

Data were collected from hospital organizations in western New York using a survey instrument. We met with hospital administrators to learn about extreme events in the region. We learned that although hospitals in the region frequently experienced outages, the duration of the outages was usually only 1 to 2 h. We further learned that outages that lasted at least 24 h constituted a state of emergency due to their negative impact on hospital workflows. For these reasons, we limited our study scenario to a 24-h unplanned outage of hospital systems (such as clinical systems, electronic medical record systems, and other administrative systems used in the provision of services). During an unplanned outage, hospital systems are not accessible to the hospital staff. The study population for our research were clinical and non-clinical staff who use hospital systems to provide direct or indirect patient services. This population was targeted because the research sought to gather opinions from employees whose work would be severely impaired by a 24-h system outage.

The survey was physically administered to healthcare workers of 8 different hospitals. The criteria for selecting hospitals were that they used health information technologies to deliver patient services, and that they had experienced system outages previously. The criteria for the respondents were that they were 18 years or older, and provided direct or indirect patient care services at one of the 8 hospitals. At the beginning of the survey, participants were informed of the study scenario. Specifically, participants were asked to answer questions based on how they are likely to respond when the hospital systems are back online following an unplanned 24 h outage. The definitions of an unplanned outage and hospital information systems were also provided.

We followed a systematic approach in developing the survey and collecting the data. First, prior to data collection, the content of the survey was validated by a subject matter expert. Second, the survey instrument was revised based on the expert's comments. Third, because data were collected from eight hospitals, we had to verify the homogeneity of the population sampled. Homogeneity was verified by examining common characteristics among the participating hospitals. Individuals signal their membership in a group through common attributes, such as associations, rules, and ethos, which consequently lead to common beliefs and values (McCurdy, 2006; Muniz et al., 2001). Accordingly, we assumed sample homogeneity based on the common attributes shared among the hospitals (see Appendix Table 2).

4.2 Operationalization of Constructs

Where possible, we adopted measurement scales from prior literature. All items in the survey were measured using a 7-point Likert scale, ranging from 1 (strongly disagree) to 7 (strongly agree). The complete measurement instrument is provided in Appendix Table 3.

4.3 Sample

A total of 600 surveys were administered to hospital employees. Prior to analyzing the data, the returned surveys were checked for completeness. Missing data were detected using the guidelines described by Hair, Hult, Ringle, and Sarstedt (2021, p. 51). After removing incomplete surveys, a total of 163 surveys remained. The sample consisted of 38 male and 121 female respondents. Four participants did not report their gender. The sample included 111 (68.53%) clinical staff members and 50 (30.86%) non-clinical staff. The majority of participants ($n = 147$) had no prior experience with disasters. The duration of work experience reported by most non-clinical participants was between 1 and 5 years. Appendix Table 4 provides a summary of the descriptive statistics.

4.4 Data Analysis

Power Analysis We performed a power analysis to verify that the sample size was adequate for detecting a particular effect. The power analysis was performed based on the guidelines described by Hair, Ringle, and Sarstedt (2011, p. 20). With six variables, the sample size of 163 met the required minimum for obtaining a statistical power of 80 percent, and an R square value of at least 0.25 at a p value of less than 0.05 was detected.

Validity and Reliability The measurement scale was evaluated for reliability and validity. Internal consistency and item reliability were assessed according to the criteria given by Podsakoff, MacKenzie, Lee, and Podsakoff (2003, pp. 96–107). Appendix Table 5 provides the results for the validity and reliability analysis. As seen in Appendix Table 5, the recommended psychometric properties of the scale were met.

Partial Least Squares – Structural Equation Modeling (PLS-SEM) Regression The hypothesized relationships were tested using PLS-SEM version 3.2.1 (Ringle, Wende, & Becker, 2014). The bootstrapping procedure was run with

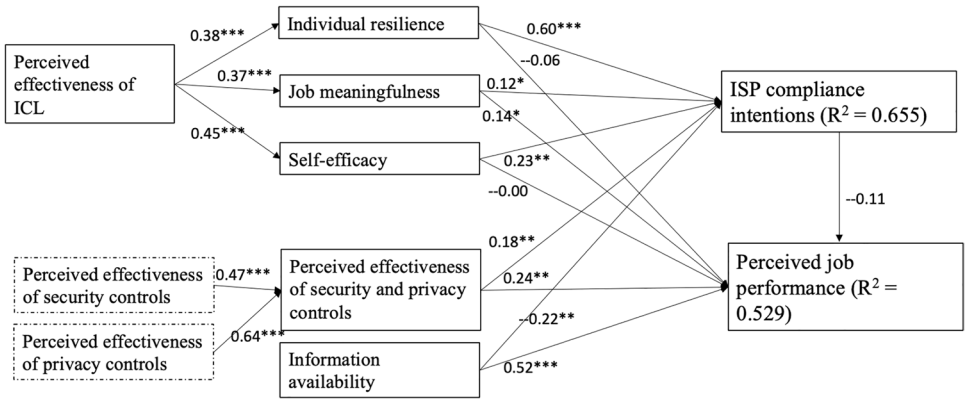

Fig. 2 Results of the hypothesized model of the factors that inclluence perceived job performance during extreme events. Path significance: *$p < 0.05$, **$p < 0.01$, ***$p < 0.000$

Table 1 Results summary of support for hypotheses

Path	β	*t*-value	*Supported?*
Individual resilience ➔ ISP compliance intentions	0.60	10.68***	Yes
Individual resilience ➔ Perceived job performance	-0.06	0.978	No
Job meaningfulness ➔ ISP compliance intentions	0.12	1.931*	Yes
Job meaningfulness ➔ Perceived job performance	0.14	2.109*	Yes
Self-efficacy ➔ ISP compliance intentions	0.23	2.836**	Yes
Self-efficacy ➔ Perceived job performance	-0.00	0.00	No
Perceived effectiveness of ICL ➔ Individual resilience	0.38	5.655***	Yes
Perceived effectiveness of ICL ➔ Job meaningfulness	0.37	5.412***	Yes
Perceived effectiveness of ICL ➔ Self-efficacy	0.45	6.355***	Yes
Perceived effectiveness of security and privacy controls ➔ ISP compliance intentions	0.18	2.363**	Yes
Perceived effectiveness of security and privacy controls ➔ Perceived job performance	0.24	2.662**	Yes
Information availability ➔ ISP compliance intentions	-0.22	2.586**	Yes
Information availability ➔ Perceived job performance	0.52	4.291***	Yes
Perceived effectiveness of security controls ➔ Perceived effectiveness of security and privacy controls	0.47	17.880***	Yes
Perceived effectiveness of privacy controls ➔ Perceived effectiveness of security and privacy controls	0.64	18.373***	Yes
ISP compliance intentions ➔ Perceived job performance	-0.11	1.319	No

Path significance: *$p < 0.05$, **$p < 0.01$, ***$p < 0.000$

5,000 subsamples and with individual sign changes. The decision to use the individual sign changes option was based on criteria described in earlier work (Tenenhaus, Vinzi, Chatelin, & Lauro, 2005). The percentage of variance in the model, which is indicated by the R^2 values in Fig. 2, is 0.690 for ISP compliance intentions, and 0.528 for perceived job performance.

4.5 Results

The results of the hypothesized structural model are shown in Fig. 2. In Table 1, we provide the values for the path coefficient (β), significance (*t*-value), and *p*-value from SmartPLS 3.2.1 (Bido et al., 2014). Hypotheses 1a, 2a, 2b, 3a, 4a,4b, 4c, 5a, 5b, and 6b were all supported. The results showed that during extreme events, both psychological and organizational resources significantly influenced ISP compliance decisions as follows: individual resilience had the strongest effect, at b = 0.60, $p < 0.00$, followed by self-efficacy at b = 0.23, $p < 0.01$, perceived effectiveness of security and privacy controls at b = 0.18, $p < 0.01$, and lastly, job meaningfulness at b = 0.12, $p < 0.05$. These results suggest that an employee's ability to cope under pressure is a stronger determinant of compliance decisions compared to organizational resources, such as security controls. The hypothesized relationship between information availability

and ISP compliance intentions was supported, but in the opposite direction.

The data also showed that during extreme events, perceived job performance was significantly influenced by both psychological and organizational resources. The strongest predictor of perceived job performance was information availability, at b = 0.52, $p < 0.00$, followed by perceived effectiveness of security and privacy controls at b = 0.24, $p < 0.01$, and lastly, job meaningfulness at b = 0.14, $p < 0.05$. The relationship between ISP compliance intentions and perceived job performance was not significant, b = -0.11, p < 0.1. The hypothesized effects of individual resilience and self-efficacy were not significant. These findings seem to suggest that during extreme events, organizational resources are more integral than psychological resources to achieving enhanced job performance.

Also, the perceived effectiveness of ICL strengthens individual resilience, job meaningfulness, and perceived self-efficacy, indicating that even during extreme events, leadership still plays a critical role in motivating employees to engage in positive work behaviors.

4.6 Post Hoc Analysis

We conducted a post hoc analysis following the initial study to examine the perceptions of employees who had experienced an extreme event while at work. We sought to study the hypothesized variables and to examine their influence on perceived job performance during a real extreme event. Data for the post hoc analysis was collected through Amazon Mechanical Turk (MTurk), an online platform with verified participants aged 18 years or older. Respondents were asked to answer questions based on the extreme event they had experienced while working. A sample size of 188 employees in the healthcare industry were analyzed, and the results are shown in Fig. 3. The results showed that ISP compliance intentions were strengthened by only one of the three psychological resources studied—namely, self-efficacy—and one organizational resource: the perceived effectiveness of security and privacy controls. Individual resilience, job meaningfulness, and information availability had no significant effect on ISP compliance intentions among respondents. With respect to job performance, individual resilience and information availability *did* have a positive relationship with perceived job performance. Not surprisingly, we found that the perceived effectiveness of security and privacy controls had a negative influence on job performance. The relationship between ISP compliance intentions and perceived job performance was not significant.

5 Discussion

5.1 Research Contributions and Implications

The findings in this study broaden our understanding of ISP compliance when the work environment is operating during extreme events. Existing research has extensively studied ISP compliance under normal working conditions, with little or no attention paid to how compliance decisions may change when employees are experiencing strain. We used the COR theory to offer an alternative perspective, hypothesizing that when working under strain, employees are confronted with performing their job tasks efficiently and effectively, while still complying to ISP. The demands of ISP compliance can be addressed by applying not only organizational resources, which have previously been studied in isolation, but psychological resources as well, which are vital to coping with unexpected events in the workplace.

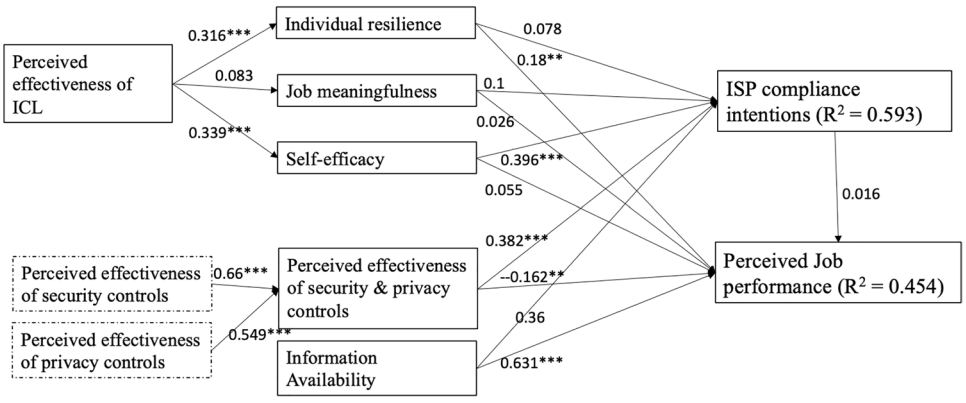

Fig. 3 Results of the post hoc analysis of the factors that influence perceived job performance amongst respondents who have experienced an extreme event. Path significance: *$p < 0.05$, **$p < 0.01$, ***$p < 0.000$

Our findings showed that psychological resources—namely, individual resilience, job meaningfulness, and self-efficacy—significantly increase ISP compliance intentions.

Our research shows that employees experiencing strain still possess strong ISP compliance intentions, *if* they are highly resilient. The results also demonstrated that job meaningfulness gives an employee a sense of hope that their work has value to the organization. As such, employees who find purpose in their work will view ISP compliance as a valuable behavior for contributing to the organization's overall security objectives. In regard to self-efficacy, we confirmed earlier findings, such as by Chan et al. (2005) and Herath and Rao (2009a), about the relationship between self-efficacy and ISP compliance. We showed that employees' belief in their ability to successfully complete work tasks increases their intentions to comply with ISP. These findings indicate that even during extreme events, perceived self-efficacy motivates employees to engage in desired security behaviors, such as ISP compliance.

However, the hypothesized psychological resources did not result in increased job performance, with the exception of job meaningfulness. It appears that when faced with extreme events, employees focus their psychological resources (i.e., resilience and competency) on compliance instead of job performance. In particular, individual resilience did not have a significant impact on perceived job performance. A potential explanation for this finding can be found in the management literature, which explains that resilience may not always bring about positive outcomes (Kaplan & Kaiser, 2009; Paton et al., 2000; Pierce & Aguinis, 2013). The literature explains that personal resources can produce desired work outcomes; however, overusing such resources can result in undesirable outcomes (Kaplan & Kaiser, 2009). It is also plausible that when employees are confronted with more than one job responsibility, personal strengths, such as resilience and self-efficacy, introduce the risk of an unbalanced resource expenditure such that increased efficiency and effectiveness in one area lead to diminished efficiency and productivity in other areas. Another possible explanation for why individual resilience can predict ISP compliance intentions but not perceived job performance can be found in Treglown et al. (2016). The authors determined that resilience was negatively associated with cautiousness. Our data were collected from hospital workers charged with the responsibility of complying with HIPAA regulations and providing high-quality care services to patients at all times. Treglown et al. (2016) supported the notion that extreme events, resilient employees will approach care delivery with caution in order to limit the likelihood of errors, which could result in patient deaths. Similarly, we observed the tradeoff between ISP compliance and perceived job performance regarding self-efficacy. ISP compliance comes at the expense of job performance for employees with strong self-efficacy. Overall, these findings confirm recent observations in (Shin & Grant, 2019) that when individuals are intrinsically motivated to perform one task, the motivation to perform other tasks wanes.

Three organizational resources were included in our research model: perceived effectiveness of ICL, perceived effectiveness of security and privacy controls, and information availability. Our results suggest that during extreme events in the workplace, leadership strengthens individual resilience, job meaningfulness, and self-efficacy. This finding furthers our understanding of the role of leadership by showing that a well-defined command and control structure for managing turbulence in the workplace is essential for achieving desired security and performance goals. Existing research has shown that resilience is developed through hardship (Mitchell et al., 2019; Williams et al., 2017). We built on these findings by demonstrating that an employee's resilience can also be constructed through effective leadership. For example, effective leadership can inspire employees with little or no resilience to develop the resiliency needed to overcome adversity, consequently increasing their likelihood for ISP compliance. Likewise, leaders can intervene when they observe employees engaging in unfavorable security behavior by applying interventions (e.g., training) to improve job meaningfulness and self-efficacy.

We suspected that the perceived effectiveness of security and privacy controls contributes positively to perceived job performance. Effective controls communicate the importance of security to the organization. When existing controls are able to successfully safeguard information resources, employees are encouraged to engage in security and privacy risk mitigation behaviors, such as ISP compliance.

Lastly, as hypothesized, information availability predicted perceived job performance. The data showed that the availability of information pertaining to the disturbance, and the information needed to perform work tasks, lower compliance intentions. This negative relationship could be attributed to the possibility of information overload (Eppler & Mengis, 2004). Frequent information updates about a disruption in the workplace can easily become a barrier to performance if the volume of updates is perceived to be excessive. In the context of ISP compliance, excessive information may

culminate in confusion and performance pressure, consequently reducing ISP compliance intentions. This finding informs the security compliance literature about the significant negative relationship between information availability and ISP compliance decisions during extreme events. Overall, this research extended the COR theory to identity the resources essential to job performance during extreme events. During normal working conditions, the tenants of the standard COR theory should still be supported.

5.2 Implications from the Post Hoc Analysis

The results from the post hoc analysis offer several implications for managing job performance during extreme events. First, we determined that during extreme events, security and privacy procedures impede productivity but not ISP compliance. This implies that during tumultuous working conditions, tasking employees with responsibilities related to security and privacy reduces their performance and productivity in other areas, such as providing customer services. Second, the impact of self-efficacy on ISP compliance intentions was stronger for respondents who had experienced an actual extreme event while at work than for respondents in the original sample. Employees who feel confident in their ability to manage security tasks are likely to comply with ISP and also to manage other work-related tasks, even when working during extreme events. Third, individual resilience significantly increased perceived job performance, but it had no effect on ISP compliance intentions. This suggests that during an extreme event, when an organization is operating under strain, employees will use their resilience capital on work tasks that are not related to security and privacy. Fourth, the availability of and access to timely information significantly improves employee job performance during extreme events.

Overall, findings from the post hoc analysis offer valuable insights into security management, and about business continuity managers. One recommendation in this regard is to automate security and privacy tasks to reduce employee responsibilities and workload while also promoting high performance in non-security tasks. Also, organizations are encouraged to promote psychological resources—specifically, self-efficacy and individual resilience—to motivate ISP compliance and job performance, respectively. These psychological resources can be strengthened during extreme events through incident command leadership.

5.3 Implications to Practice

As articulated in this research, privacy vs. utility is a trade-off and in the hospital context, the health and safety of patients and medical staff is a trade-off with patient privacy. As is evident from the current Covid-19 pandemic, while it is critical for patient information to be protected, it is equally important for it to be adequately shared to protect healthcare workers from being infected. Similarly, in case of a mass casualty event (e.g. school shootings) it is more critical to save victims than to protect their privacy. If possible, patient information should be protected, however, patient care should take precedence in situations where privacy rules impede the delivery of critical care services. Such flexibility should be codified in the hospital disaster response operational handbooks so as not to leave employees conflicted. Also, as information availability becomes key to both job performance as well as to security, access to information should become easier. For instance, dual authentication to access information can be suspended during extreme events such that Health Information Exchanges can share patient information with emergency attending physicians without requiring extensive approval protocols. Additionally, the benefits of security and privacy controls should be clearly communicated to the healthcare workers so that they can make more informed judgments on the merits of loosening privacy constraints (during extreme events). Finally, table top crisis exercises should include security and privacy protocols so that healthcare workers perceive high levels of self-efficacy in managing security and privacy protocols during hospital emergencies.

5.4 Limitations and Future Research

Our study has some limitations. First, the data were collected using a survey instrument from healthcare organizations. As such, the findings may not be generalizable to other industries. Therefore, future research is needed to test the hypothesized model using generalizable data from other industries, such as banking and manufacturing. Second, the disturbance studied was a power outage. Further research is needed on other types of emergency events that might trigger different psychological responses from employees.

Another area for future research relates to the negative influence of information availability on ISP compliance decisions. It is known that information contributes positively to employee performance only to a certain point, beyond which overload will result (Eppler & Mengis, 2004). What is not known, however, is how much is *too much* information for employees when working under strain induced by extreme events. Another factor to consider in future studies is how to present and/or disseminate information to employees without disrupting performance and ISP compliance decisions.

Also, more research is needed to better our understanding of how psychological factors influence performance tasks. Our research made observations similar to those found in (Shin & Grant, 2019) regarding the tradeoff employees make by focusing their strengths on one task at the expense of others. However, this is not true for all psychological factors, as we found in this study. Further research is needed to identify which other psychological factors (besides job meaningfulness) are not susceptible to individual performance tradeoffs.

6 Conclusion

In contemporary organizations, employees are expected to not only perform their jobs well but also to comply with ISP during extreme events. This research furthers our understanding of job performance by revealing which factors influence ISP compliance intentions and how such intentions influence job performance when stress induced by an extreme event occurs in the workplace. We hypothesized that both psychological and organizational resources are essential to strengthening employees' ISP compliance intentions and perceived job performance. Overall, our findings suggest that during extreme events, employees' priorities will change such that considerable tradeoffs between security and job performance are made. We determined that when employees are working during extreme events, they care more about ISP compliance than job performance, in some cases. For instance, individual resilience and self-efficacy significantly strengthen ISP compliance intentions but have no effect on perceived job performance. Conversely, information availability significantly improves perceived job performance but not ISP compliance intentions. Also, job meaningfulness and the perceived effectiveness of information security and privacy controls have a significant impact on both ISP compliance intentions and perceived job performance.

Our work confirms recent findings suggesting that individual motivation to accomplish a specific task reduces performance on other tasks (Shin & Grant, 2019). We observed that the motivation for ISP compliance reduces the motivation for job performance for individuals with high resilience and high self-efficacy. However, this was not the case with all intrinsic motivators, as our results indicate. For example, job meaningfulness strengthened both ISP compliance intentions and job performance, indicating that when work is perceived to be purposeful, employees will strive to meet all of the organization's goals without making performance tradeoffs between tasks.

Findings from the post hoc study suggest that ISP compliance requirements act as barriers to job performance during extreme events. However, organizations can still achieve compliance by cultivating employee self-efficacy in security tasks and by improving the effectiveness of security and privacy controls. Self-efficacy can be established and reinforced through tabletop security exercises and frequent security training. Also, automating some of the security and privacy procedures may alleviate the burden of managing security during extreme events, thereby increasing the likelihood of ISP compliance while at the same time promoting enhanced job performance and productivity in other areas.

Appendix

Appendix 1

Table 2 Attributes of participating hospitals

Hospital	Number of beds	Specialty services provided	Emergency care?	Catholic healthcare ministry affiliation?
Hospital 1	133	1	No	No
Hospital 2	175	Multiple specialties	Yes	Yes
Hospital 3	457	Multiple specialties	Yes	Yes
Hospital 4	70	Multiple specialties	Yes	Yes
Hospital 5	262	Multiple specialties	Yes	No
Hospital 6	413	Multiple specialties	Yes	Yes
Hospital 7	602	Multiple specialties	Yes	No
Hospital 8	261	Multiple specialties	Yes	Yes

Appendix 2

Table 3 Survey instrument

Construct	Items	Citation
ISP compliance intentions	1: After the extreme event (when the Health Information System (HIS) comes back online), I intend to carry out my responsibilities prescribed in the information PRIVACY POLICIES of my hospital when I use information and computers 2: After the extreme event, I intend to comply with the requirements of the information SECURITY POLICY of my hospital in the future 3: After the extreme event, I intend to protect information and technology resources according to the requirements of the information SECURITY POLICY of my hospital in the future 4: After the extreme event, I intend to comply with the requirements of the information PRIVACY POLICY of my hospital in the future 5: After the extreme event, I intend to maintain the privacy of information and technology resources according to the requirements of the information PRIVACY POLICY of my hospital in the future	(Bulgurcu et al., 2010)
Perceived Job Performance	Immediately after the extreme event (when the HIS comes back online), I would be… 1: …. able to perform my duties on time 2: …. able to respond to patient requests promptly 3: …. able to give individual attention to patients	(Cronin Jr & Taylor, 1992)
Individual resilience	1: I would bounce back quickly after the extreme event 2: It would not take me long to recover from the extreme event 3: I would come through the extreme event with little trouble	(Smith et al., 2008)
Job meaningfulness	1: Immediately after the extreme event, I feel that the work I do would be very important to me 2: Immediately after the extreme event, I feel that my job activities would be personally meaningful to me	(Spreitzer, 1995)
Perceived self- efficacy	1: Immediately after the extreme event (when the HIS come back online), I would be confident in my ability to recognize security and privacy risks to patients' information 2: Immediately after the extreme event (when the HIS come back online), I would be confident in my ability to maintain the privacy of patients' information at all times 3: Immediately after the extreme event (when the HIS come back online), I would be confident in my ability to keep patients' information secure	N/A
Perceived effectiveness of ICL	Item 1: There is a leader who oversees and manages activities Immediately after the extreme event (when the HIS comes back online), the leader would. 2:.. provide me with clear instructions 3:.. be available to respond to my questions 4:.. be encouraging and supportive 5:.. allow me to make decisions	(MacKenzie et al., 2001)
Perceived effectiveness of privacy controls	1: My hospital would have sufficient controls for safeguarding the privacy of patients' information after the extreme event 2: My hospital would have policies for safeguarding the privacy of patients' information after the extreme event 3: My hospital would have workflows for safeguarding the privacy of patients' information after the extreme event	N/A
Perceived effectiveness of security policies	1: Immediately after the extreme event (when the HIS comes back online), the Hospital Information Systems (HIS) would make it possible for me to securely share information within the hospital 2: Immediately after the extreme event (when the HIS comes back online), the Hospital Information Systems (HIS) would make it possible for me to securely share information with individuals outside the hospital 3: Immediately after the extreme event (when the HIS comes back online), the (HIS) would prevent unauthorized access to patients' information	N/A
Information Availability	1: Immediately after the extreme event the information I need to do my job would be made available to me 2: Immediately after the extreme event real-time information regarding the extreme event (such as resource availability, the status of electronic systems, etc., would be made available to me 3: Immediately after the extreme event (when the HIS come back online), I would have access to up-to-date information	(MacKenzie et al., 2001)

Appendix 3

Table 4 Descriptive statistics ($n = 163$)

Respondent Groups	Number of Respondents
Work group	
Clinical staff	111
Nonclinical staff	50
Gender	
Women	121
Men	38
Leadership role	
Managers	36
Non-managers	126
Role during emergencies	
Leadership role	26
Non-leadership role	135

Appendix 4

Table 5 Validity and Reliability Results

Variable/Items	Item loading	Cronbach alpha	Composite reliability	AVE
ISP compliance intentions		0.942	0.956	0.812
1	0.836			
2	0.867			
3	0.941			
4	0.923			
5	0.935			
Perceived Job Performance		0.937	0.960	0.888
1	0.937			
2	0.953			
3	0.937			
Individual resilience		0.747	0.839	0.648
1	0.814			
2	0.815			
3	0.786			
Job meaningfulness		0.919	0.961	0.925
1	0.965			
2	0.958			
Perceived self- efficacy		0.918	0.948	0.860
1	0.896			
2	0.953			
3	0.931			
Perceived effectiveness of ICL(		0.964	0.962	0.844
1	0.887			
2	0.950			
3	0.948			
4	0.942			
5	0.863			
Perceived effectiveness of security and privacy controls (second-order construct)		0.921	0.939	0.719
Perceived effectiveness of privacy controls		0.909	0.943	0.847
1	0.877			
2	0.941			
3	0.942			
Perceived effectiveness of security policies		0.759	0.862	0.678
1	0.903			
2	0.792			
3	0.767			
Information Availability		0.914	0.945	853
1	0.929			
2	0.932			
3	0.909			

Declarations

Conflict of Interests There are no financial and non-financial conflict of interests in context of this paper.

References

Ab Rahman, N. H., and Choo, K.-K. R. (2015). A Survey of Information Security Incident Handling in the Cloud. *Computers & Security* (49): 45–69.

Abramson, D. M., & Redlener, I. (2012). Hurricane Sandy: Lessons Learned, Again. *Disaster Medicine and Public Health Preparedness, 6*(4), 328–329.

Ahmad, A., Hadgkiss, J., & Ruighaver, A. B. (2012). Incident Response Teams-Challenges in Supporting the Organisational Security Function. *Computers & Security, 31*(5), 643–652.

Ahmad, A., Maynard, S. B., & Shanks, G. (2015). A Case Analysis of Information Systems and Security Incident Responses. *International Journal of Information Management, 35*(6), 717–723.

Ajzen, I. (1985). From Intentions to Actions: A Theory of Planned Behavior, in *Action Control: From Cognition to Behavior,* J. Kuhl and J. Beckmann (eds.). Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 11–39.

Ajzen, I. (1991). The Theory of Planned Behavior. *Organizational Behavior and Human Decision Processes, 50*(2), 179–211.

Anderson, C. R. (1977). Locus of Control, Coping Behaviors, and Performance in a Stress Setting: A Longitudinal Study. *Journal of Applied Psychology, 62*(4), 446.

Arshadi, N., & Damiri, H. (2013). The Relationship of Job Stress with Turnover Intention and Job Performance: Moderating Role of Obse. *Procedia-Social and Behavioral Sciences, 84,* 706–710.

Barth, A., Mitchell, J., Datta, A., & Sundaram, S. (2007). Privacy and utility in business processes. *In 20th IEEE Computer Security Foundations Symposium (CSF'07)*(pp 279-294). IEEE

Baskerville, R., Spagnoletti, P., & Kim, J. (2014). Incident-Centered Information Security: Managing a Strategic Balance between Prevention and Response. *Information & Management, 51*(1), 138–151.

Bauer, S., Bernroider, E. W., and Chudzikowski, K. (2017). Prevention Is Better Than Cure! Designing Information Security Awareness Programs to Overcome Users' Non-Compliance with Information Security Policies in Banks. *Computers & Security* (68) 145–159.

Beaudry, A. (2009). Coping with Information Technology, in *Handbook of Research on Contemporary Theoretical Models in Information Systems*. IGI Global, pp. 516–528.

Beaudry, A., and Pinsonneault, A. (2005). Understanding user responses to information technology: A coping model of user adaptaion. *MIS Quarterly, 29*(3), 493–524. https://doi.org/10.2307/25148693.

Bharosa, N., Lee, J., & Janssen, M. (2010). Challenges and Obstacles in Sharing and Coordinating Information During Multi-Agency Disaster Response: Propositions from Field Exercises. *Information Systems Frontiers, 12*(1), 49–65.

Bido, D., da Silva, D., & Ringle, C. (2014). Structural Equation Modeling with the Smartpls. *Brazilian Journal Of Marketing, 13*(2). Retrieved October 19, 2015

Britt, T. W., Adler, A. B., & Bartone, P. T. (2001). Deriving Benefits from Stressful Events: The Role of Engagement in Meaningful Work and Hardiness. *Journal of Occupational Health Psychology, 6*(1), 53.

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.

Carton, A. M. (2018). "I'm Not Mopping the Floors, I'm Putting a Man on the Moon": How Nasa Leaders Enhanced the Meaningfulness of Work by Changing the Meaning of Work. *Administrative Science Quarterly, 63*(2), 323–369.

Cascio, W. F. (2003). Changes in workers, work, and organizations. In W. C. Borman, D. R. Ilgen, & R. J. Klimoski (Eds.), *Handbook of psychology: Industrial and organizational psychology* (vol 12, pp 401–422). John Wiley & Sons Inc

Chakraborty, S., Raghavan, K. R., Johnson, M. P., & Srivastava, M. B. (2013). A framework for context-aware privacy of sensor data on mobile systems. *In Proceedings of the 14th Workshop on Mobile Computing Systems and Applications* (pp 1–6).

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 and Security, 1*(3), 18–41.

Charbonneau, D., Barling, J., & Kelloway, E. K. (2001). Transformational Leadership and Sports Performance: The Mediating Role of Intrinsic Motivation 1. *Journal of Applied Social Psychology, 31*(7), 1521–1534.

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.

Clarke, S. (2006). The relationship between safety climate and safety performance: a meta-analytic review. *Journal of occupational health psychology, 11*(4), 315

Cronin. Jr, J. & Taylor, Steve. (1992). Measuring service quality - a reexamination and extension. *The Journal of Marketing, 56*, 55–68. https://doi.org/10.2307/1252296.

Devitt, K. R., & Borodzicz, E. P. (2008). Interwoven Leadership: The Missing Link in Multi-Agency Major Incident Response. *Journal of Contingencies and Crisis Management, 16*(4), 208–216.

Eppler, M. J., & Mengis, J. (2004). The Concept of Information Overload: A Review of Literature from Organization Science, Accounting, Marketing, Mis, and Related Disciplines. *The Information Society, 20*(5), 325–344.

Erez, A., & Judge, T. A. (2001). Relationship of Core Self-Evaluations to Goal Setting, Motivation, and Performance. *Journal of Applied Psychology, 86*(6), 1270.

Federal Emergency Management Agency. (2010). Developing and Maintaining Emergency Operations Plans. Federal Emergency Management Agency.

Federal Emergency Management Agency. (2018). Ics Review Document—Extracted from E/L/G 0300 Intermediate Incident Command System for Expanding Incidents, Ics 300.

Federal Emergency Management Agency. (2019). National Incident Management System. Federal Emergency Management Agency.

Fletcher, D., & Sarkar, M. (2013). Psychological Resilience: A Review and Critique of Definitions, Concepts, and Theory. *European Psychologist, 18*(1), 12.

Goel, S. (2015). Anonymity vs. security: The right balance for the smart grid. *Communications of the Association for Information Systems, 36*(1), 2.

Hair Jr, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2021). A primer on partial least squares structural equation modeling (PLS-SEM). Sage publications.

Hair, J. F., Ringle, C. M., & Sarstedt, M. (2011). PLS-SEM: Indeed a silver bullet. *Journal of Marketing theory and Practice, 19*(2), 139–152.

Halperin, D., Heydt-Benjamin, T. S., Fu, K., Kohno, T., & Maisel, W. H. (2008). Security and privacy for implantable medical devices. *IEEE pervasive computing, 7*(1), 30–39.

Hannah, S. T., Schaubroeck, J. M., & Peng, A. C. (2016). Transforming Followers' Value Internalization and Role Self-Efficacy: Dual Processes Promoting Performance and Peer Norm-Enforcement. *Journal of Applied Psychology, 101*(2), 252.

Herath, T., & Rao, H. R. (2009). Encouraging Information Security Behaviors in Organizations: Role of Penalties, Pressures and Perceived Effectiveness. *Decision Support Systems, 47*(2), 154–165.

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.

Hiller, M., Bone, E. A., & Timmins, M. L. (2015). Healthcare System Resiliency: The Case for Taking Disaster Plans Further—Part 2. *Journal of Business Continuity & Emergency Planning, 8*(4), 356–375.

Hobfoll, S. E. (1989). Conservation of Resources: A New Attempt at Conceptualizing Stress. *American Psychologist, 44*(3), 513.

Hobfoll, S. E. (2002). Social and Psychological Resources and Adaptation. *Review of General Psychology, 6*(4), 307–324.

Hove, C., Tårnes, M., Line, M. B., and Bernsmed, K. (2014). Information Security Incident Management: Identified Practice in Large Organizations, *2014 Eighth international conference on IT security incident management & IT forensics*: IEEE, pp. 27–46.

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), 615–660.

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. (2014). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialisation, Influence, and Cognition. *Information & Management, 51*(1), 69–79.

Järveläinen, J. (2013). It Incidents and Business Impacts: Validating a Framework for Continuity Management in Information Systems. *International Journal of Information Management, 33*(3), 583–590.

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

Kam, H.-J., Mattson, T., & Goel, S. (2020). A Cross Industry Study of Institutional Pressures on Organizational Effort to Raise Information Security Awareness. *Information Systems Frontiers, 22*(5), 1241–1264.

Kaplan, R. E., & Kaiser, R. B. (2009). Stop Overdoing Your Strengths. *Harvard Business Review, 87*(2), 100–103.

Karimi, R., & Alipour, F. (2011). Reduce Job Stress in Organizations: Role of Locus of Control. *International Journal of Business and Social Science, 2*(18), 232–236.

Kweon, E., Lee, H., Chai, S., & Yoo, K. (2021). The Utility of Information Security Training and Education on Cybersecurity Incidents: An Empirical Evidence. *Information Systems Frontiers, 23*(2), 361–373.

Liang, H., & Xue, Y. (2009). Avoidance of information technology threats: A theoretical perspective. *MIS Quarterly, 33*, 71–90. https://doi.org/10.2307/20650279

Lowe, K. B., Kroeck, K. G., & Sivasubramaniam, N. (1996). Effectiveness correlates of transformational and transactional leadership: A meta-analytic review of the MLQ literature. *The leadership quarterly, 7*(3), 385–425.

MacKenzie, S. B., Podsakoff, P. M., & Rich, G. A. (2001). Transformational and Transactional Leadership and Salesperson Performance. *Journal of the Academy of Marketing Science, 29*(2), 115–134.

Maslach, C., Schaufeli, W. B., & Leiter, M. P. (2001). Job Burnout. *Annual Review of Psychology, 52*(1), 397–422.

McCurdy, D. W. (2006). Using anthropology. *Conformity and conflict* (12th ed., pp 422–435). Allyn and Bacon Publishers

Mitchell, M. S., Greenbaum, R. L., Vogel, R. M., Mawritz, M. B., & Keating, D. J. (2019). Can You Handle the Pressure? The Effect of Performance Pressure on Stress Appraisals, Self-Regulation, and Behavior. *Academy of Management Journal, 62*(2), 531–552.

Mitropoulos, S., Patsos, D., & Douligeris, C. (2006). On Incident Handling and Response: A State-of-the-Art Approach. *Computers & Security, 25*(5), 351–370.

Morgeson, F. P., Garza, A. S., & Campion, M. A. (2012). Work design. *Handbook of Psychology* (2nd ed., vol 12, pp 318–327).

Morrison, J. L., Titi Oladunjouye, G., & Dembry, D. (2014). An assessment of Ceo oversight of natural disaster preparedness. *International Journal of Business & Public Administration, 11*(1), 66–81.

Muniz, J., Albert, M., & O'Guinn, T. C. (2001). Brand Community. *Journal of Consumer Research, 27*(4), 412–432.

Ng, T. W., Sorensen, K. L., & Eby, L. T. (2006). Locus of Control at Work: A Meta-Analysis. *Journal of Organizational Behavior: The International Journal of Industrial, Occupational and Organizational Psychology and Behavior, 27*(8), 1057–1087.

Ong, A. D., Bergeman, C. S., Bisconti, T. L., & Wallace, K. A. (2006). Psychological Resilience, Positive Emotions, and Successful Adaptation to Stress in Later Life. *Journal of personality and social psychology, 91*(4), 730.

Pahnila, S., Siponen, M., and Mahmood, A. (2007). "Employees' Behavior Towards Is Security Policy Compliance," *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*: IEEE, pp. 156b-156b.

Paton, D., Smith, L., & Violanti, J. (2000). Disaster Response: Risk, Vulnerability and Resilience. *Disaster Prevention and Management: An International Journal, 9*(3), 173–180.

Pierce, J. R., & Aguinis, H. (2013). The Too-Much-of-a-Good-Thing Effect in Management. *Journal of Management, 39*(2), 313–338.

Podsakoff, P. M., MacKenzie, S. B., Lee, J. Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of applied psychology, 88*(5), 879.

Puhakainen, P., and Siponen, M. (2010). Improving Employees' Compliance through Information Systems Security Training: An Action Research Study. *Mis Quarterly*. 757–778.

Rainie, L., & Duggan, M. (2016). Privacy and information sharing. Available at https://www.pewresearch.org/internet/2016/01/14/privacy-and-information-sharing/

Ringle, C. M., Wende, S., & Becker, J. M. (2014). SmartPLS 3. Hamburg: SmartPLS. *Academy of Management Review, 9*, 419–445.

Roberts, P. (2006). Fema after Katrina. *Policy Review, 137*(June&July), 15–33.

Rosso, B. D., Dekas, K. H., & Wrzesniewski, A. (2010). On the Meaning of Work: A Theoretical Integration and Review. *Research in Organizational Behavior, 30,* 91–127.

Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information Security Policy Compliance Model in Organizations. *Computers & Security* (56):70–82.

Sankar, L., Rajagopalan, S. R., & Poor, H. V. (2013). Utility-privacy tradeoffs in databases: An information-theoretic approach. *IEEE Transactions on Information Forensics and Security, 8*(6), 838–852.

Scarinci, C. A. (2014). Contingency Planning and Disaster Recovery after Hurricane Sandy. *The CPA Journal, 84*(6), 60.

Shin, J., & Grant, A. M. (2019). Bored by Interest: How Intrinsic Motivation in One Task Can Reduce Performance on Other Tasks. *Academy of Management Journal, 62*(2), 415–436.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' Adherence to Information Security Policies: An Exploratory Field Study. *Information & Management, 51*(2), 217–224.

Smith, B. W., Dalen, J., Wiggins, K., Tooley, E., Christopher, P., & Bernard, J. (2008). The Brief Resilience Scale: Assessing the Ability to Bounce Back. *International Journal of Behavioral Medicine, 15*(3), 194–200.

Spector, P. E. (1982). Behavior in Organizations as a Function of Employee's Locus of Control. *Psychological Bulletin, 91*(3), 482.
Spreitzer, G. M. (1995). Psychological Empowerment in the Workplace: Dimensions, Measurement, and Validation. *Academy of Management Journal, 38*(5), 1442–1465.
Tene, O., & Polonetsky, J. (2012). Big data for all: Privacy and user control in the age of analytics. *Nw J Tech & Intell Prop, 11*, xxvii.
Tenenhaus, M., Vinzi, V. E., Chatelin, Y. M., & Lauro, C. (2005). PLS path modeling. *Computational statistics & data analysis, 48*(1), 159–205.
Tøndel, I. A., Line, M. B., & Jaatun, M. G. (2014). Information Security Incident Management: Current Practice as Reported in the Literature. *Computers & Security, 45,* 42–57.
Trang, S., & Brendel, B. (2019). A Meta-Analysis of Deterrence Theory in Information Security Policy Compliance Research. *Information Systems Frontiers, 21*(6), 1265–1284.
Treglown, L., Palaiou, K., Zarola, A., & Furnham, A. (2016). The Dark Side of Resilience and Burnout: A Moderation-Mediation Model. *PLoS One1, 11*(6), e0156279.
Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating Is Security Compliance: Insights from Habit and Protection Motivation Theory. *Information & Management, 49*(3), 190–198.
Wall, J. D., Palvia, P., & Lowry, P. B. (2013). Control-Related Motivations and Information Security Policy Compliance: The Role of Autonomy and Efficacy. *Journal of Information Privacy and Security, 9*(4), 52–79.
Whiteoak, J. W., & Mohamed, S. (2016). Employee engagement, boredom and frontline construction workers feeling safe in their workplace. *Accident Analysis & Prevention, 93*, 291–298.
Williams, T. A., Gruber, D. A., Sutcliffe, K. M., Shepherd, D. A., & Zhao, E. Y. (2017). Organizational Response to Adversity: Fusing Crisis Management and Resilience Research Streams. *Academy of Management Annals, 11*(2), 733–769.
Wu, F. T. (2013). Defining privacy and utility in data sets. *U Colo L Rev, 84*, 1117.
Yang, C.-G., & Lee, H.-J. (2016). A Study on the Antecedents of Healthcare Information Protection Intention. *Information Systems Frontiers, 18*(2), 253–263.

Victoria Kisekka , is an Assistant Professor in the Information Security and Digital Forensics department, at the University of Albany. She attained her doctoral degree from the University at Buffalo's School of management. She has published her research in high quality information systems journals and has also presented at several conferences and workshops such as the International Conference on Information Systems and the Americas Conference on Information Systems. Her research interests include security and privacy behavior, security risk, health information technologies, and emergency response and preparedness.

Sanjay Goel , is a Professor and Chair of the Information Security and Digital Forensics Department in the School of Business and the Director of the NY State Center for Information Forensics and Assurance. He is also the Director of the Digital Forensics BS and MS Programs at the University which he started. Dr. Goel received his Ph.D. in Mechanical Engineering from RPI. His research interests include information security, cyber warfare, music piracy, complex systems, security behavior, and cyber physical systems. His research on self-organizing systems includes traffic light coordination, smart grid and social networks. He is actively engaged in policy efforts on cyber security norms, CBMs, and cyber treaties. He has over 100 articles in refereed journals and conference publications including top journals. He is a recognized international expert in information security, cyber warfare, and smart grid and has given plenary talks in events across several countries. In addition, he has been invited to present at 50 conferences including over 15 keynotes and plenary talks. He established the Annual Symposium on Information Assurance and the International Conference on Digital Forensics and Cyber Crime (ICDF2C).