Finding Grace in Responses to Adverse Cybersecurity Incidents

Marc Dupuis[1], Rosalind Searle[2], Karen Renaud[3]*

[1]University of Washington, [2]University of Glasgow, [3]University of Strathclyde

*karen.renaud@strath.ac.uk

Abstract

Design/Methodology/Approach: We detail a study with 60 participants to explore attribution differences in response to adverse non-cybersecurity and cybersecurity incidents. We examined the stages that occur in the aftermath of adverse incidents where grace may be observed.

Purpose: Adverse incidents are an inescapable fact of life in organizational settings; consequences could be significant and costly. Increasingly, the cause may be a cybersecurity exploit, such as a well-targeted phishing email. In the aftermath, supervisors and managers have a choice in responding to the individual who caused the incident. Negative emotions, such as shame and regret, may deliberately be weaponized. Alternatively, positive emotions, such as grace, forgiveness and mercy, may come into play.

Findings: Our participants generally believed that grace was indicated towards those that triggered an adverse cybersecurity incident, pointing to situational causes. This was in stark contrast to their responses to the non-cybersecurity incident, where the individual was often blamed, with punishment being advocated.

Research Implications: The role of positive emotions merit investigation in the cybersecurity context if we are to understand how best to manage the aftermaths of adverse cybersecurity incidents.

Practical Implications: Organizations that mismanage aftermaths of adverse incidents by blaming, shaming and punishing those who make mistakes will hurt other employees and their organization in the long run. The resulting harm impacts the individual who made the mistake, and also the long-term health of the organization itself.

Originality/Value: This is the first study to examine the grace phenomenon in the cybersecurity context.

1 Introduction

To err is human; employee mistakes are unavoidable. This is especially true when organizations rely on employees to perform cybersecurity tasks outside their primary objectives, where they might well have exhausted their security budget (Beautement, Sasse, & Wonham, 2008) and be experiencing security fatigue (Cram, Proudfoot, & D'Arcy, 2021). How organizations choose to address adverse incidents caused by mistakes, whether *a priori* or *ex post facto*, is crucial, especially when it comes to the way errant employees are treated (Searle, Renaud, & van der Werff, 2024).

Organizations might choose to deploy fear and shame to prevent repeat occurrences, but these emotions are not without the potential for collateral damage (Dupuis, Jennings, & Renaud, 2021; Dupuis, Renaud, & Jennings, 2022; Renaud & Dupuis, 2019; Renaud, Searle, & Dupuis, 2021). Regret, on the other hand, often considered a negative emotion, surprisingly has the potential to lead to positive outcomes, helping people to learn from adverse incidents (Renaud, Dupuis, & Searle, 2022). In considering responses to adverse incidents, it is interesting to consider arguments by (Schellekens, Dillen, & Dezutter, 2020, p.371): "*religious concepts and ancient wisdom are worthwhile to study from a psychological perspective so they can be validated and contribute even more to the flourishing of humanity.*" This begs the question — which other emotions, such as forgiveness, mercy and grace, *could and should* come into play in the aftermath of adverse incidents? Could their deliberate activation contribute to the flourishing of organizations despite adverse incidents?

In this paper, we report on a study that explored the manifestation of actions grounded in decisions to grant grace in the aftermaths of non-malicious employee mistakes that trigger adverse incidents. This exploration is carried out using the lens of two fictional but plausible organizational scenarios (both non-cybersecurity and cybersecurity) in which an employee non-maliciously triggers an adverse incident that impacts not only the organization, but also their co-worker(s). The paper structure is depicted in Figure 1.

Figure 1: Paper Structure with Section Numbers

2 Related Research

In this section, we discuss the processing of a perceived wrong by one entity (*the offender*) that affects/harms another (*the aggrieved*). The existence and manifestation of different aspects in any given situation may vary, but could include, on the part of the *offender*: expressions of regret, explanation, acknowledgment of responsibility, declaration of repentance, offers of repair, and request for forgiveness (Lewicki, Polin, & Lount Jr, 2016), as well as self-forgiveness (Bufford, McMinn, Moody, & Geczy-Haskins, 2018). The aggrieved also has a choice in terms of their reactions to the offense. An alternative reaction by the offender is to refuse to acknowledge any responsibility, and thus neither apologize nor express regret. Depending on the course of action chosen by the offender, the *aggrieved's*, reactions could include: forgiveness, kindness and/or grace or recrimination ranging from the more passive holding of a grudge to more active effort to retaliate and punish (Schellekens et al., 2020). The aggrieved can also choose not to accept an apology tendered by the offender, nor to forgive the offense (Zheng, Van Dijke, Leunissen, Giurge, & De Cremer, 2016). This interplay triggers a progression that unfolds over time, and which may positively or negatively impact not just the offender and aggrieved, but also those in the wider organization that employs both (Rutigliano, Barkevich, & Hurley, 2017; Searle et al., 2024).

To lay the groundwork for our investigation, we first delineate the key concepts: grace, forgiveness, mercy and apologies.

2.1 Delineating Key Concepts

2.1.1 Offense

An offense, in our context, is defined as "*deliberate deviation of actions from safe operating procedures*" (Reason, 1995, p.1715). Such actions are likely to trigger adverse incidents which can harm the organization and/or other employees.

2.1.2 Apology

Apologies have three core elements (Schneider, 2000): (1) *acknowledgment of an injury* that damages the bonds between the offending and offended parties, and the acceptance of personal accountability for that offense, (2) *affect* – the offender must be visibly affected personally by what she or he has done, and (3) *vulnerability* – it must be offered without defense. Refusal to apologize might deter reconciliation (La Caze, 2006). An apology might not be accepted (Zheng et al., 2016), and forgiveness might not be given. However, when grace is present, the aggrieved might still choose to forgive the offender and show mercy. Fehr and Gelfand (2010) finds that apologies are most likely to lead to forgiveness when they were congruent with their self-construals. However, Zheng et al. (2016) showed that when there is a measure of cynicism perceived by the aggrieved in the offender's reactions, the apology is unlikely to be accepted.

2.1.3 Forgiveness

Forgiveness is: *experienced as a behavior, from 'moving on' to 'reconciling'; as an emotion, whether negative, such as 'letting go of hard feelings' or positive, such as 'regaining the trust'; and as a thought, whether specific to the incident and offender, such as 'forgetting what happened' or 'letting the incident be in the past', or a general attitude, such as 'understanding that no one is perfect'* (Lawler-Row, Scott, Raines, Edlis-Matityahou, & Moore, 2007, p.245).

The efficacy of forgiveness may depend on the interplay between the offender and the aggrieved (Brady, Saldanha, & Barclay, 2023), as well as the nature of the trauma inflicted by the offense, albeit unwittingly or accidentally (Akhtar, 2002). Forgiveness can be granted without apology, can be denied after an apology (Brudholm, 2020).

2.1.4 Mercy

Mercy may be described as forbearance of punishment of an individual who has committed an offense (Corlett, 2013). With mercy, a punishment that may be just and warranted is withheld. Thus, mercy implies that while potential punishment exists, it is eschewed even in the absence of grace and forgiveness (Corlett & Corlett, 2004; Murphy, 2006).

2.1.5 Grace

Grace is defined as *"an act of showing kindness, generosity, or mercy to someone who is undeserving and potentially incapable of returning the kindness shown"* (Bufford, Sisemore, & Blackburn, 2017, p.7). This implies that forgiveness will be granted and mercy bestowed. There is no suggestion that an apology is a pre-requirement for grace to be given (Hoffman, 2008). Grace therefore manifests when a fault is forgiven, and a deserved punishment withheld.

Grace is a multifaceted concept grounded in individual experiences. Schellekens, Dillen, Dewitte, and Dezutter (2021) suggest that grace has virtuous qualities including that it is freely given, even to an undeserving recipient. It therefore extends beyond fair exchange.

In all relationships, grace emerges has having transformative and liberating powers to influence individuals and change situations for the better (Schellekens et al., 2020). Grace is thus rightly considered a virtue, but, in comparison to other virtues, has received relatively little research attention (Hodge et al., 2022). This may arise, in part, as grace has previously been viewed as a religious concept, similar to forgiveness[1].

In organizations, grace is an intentional process that results in more positive emotions, commitment to the organization, reduction in fear, and improved relationships. This is an important principle of management, as articulated by Edward Deming: *"Drive out fear, so that everyone may work effectively for the company"* (Deming, 1985, p.20). In other words, when an organization and its management have a culture of grace, fear is removed as the driver of employees' actions. When this occurs, employees are more likely to focus on producing quality outcomes and to report incidents because they *do not* fear recrimination or reprisal. Organizations can thrive and generally flourish in an atmosphere of grace (Emmons, Hill, Barrett, & Kapic, 2017; Kleine, Rudolph, & Zacher, 2019), which suggests establishing a 'forgiveness climate' (Fehr & Gelfand, 2012) has clear value.

2.1.6 Summary

Figure 2 depicts the relationships between the key terms. Table 2 fleshes out the dynamics of grace from the perspectives of the offender, the aggrieved and the organization itself.

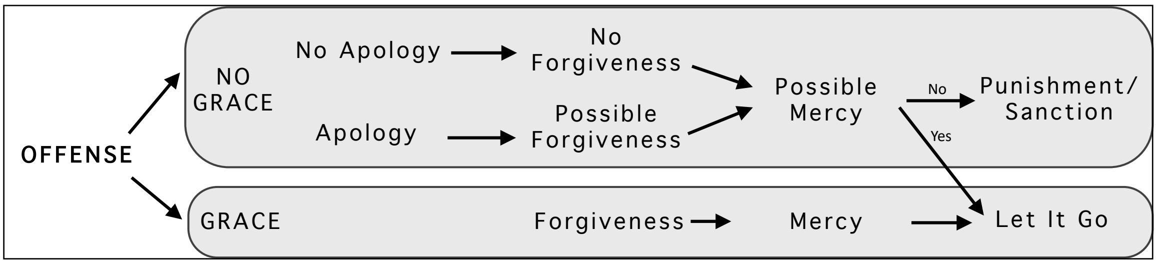

Figure 2: Core Terms and their Relationships

2.2 Stage Model of Grace

When an offense is committed, a process is triggered which will evolve over time, as decisions are made: by the offender as to whether to take responsibility, or not; by the ag-

[1] e.g., Christianity, Judaism, Islam, Hinduism) (Bufford et al., 2017). In Christianity: *"We show grace to others by forgiving those who have offended or hurt us."* (Colossians 3:13, New Living Translation Bible); in the Muslim religion: *"forgive graciously."* (Quran 15:85); Hindu devotional literature references grace (*kripa*) as the key to spiritual self-realization (The Hindu Newspaper, 2005))

OFFENDER	**AGGRIEVED**	**ORGANIZATION**
Kinds of Grace (O'Connell & Adams, 2024)		
An offender receiving grace	Aggrieved giving grace to offender	Manager giving grace to offender
Response to Offense		
Should acknowledge wrongdoing and harm by offering a genuine apology (Loszak, 2014), accept full responsibility to be enable self forgiveness h (Ong, 2023) and release themselves from self-recrimination (McConnell & Dixon, 2012). Should commit to not repeating the offense (Loszak, 2014). Must atone: act to compensate the aggrieved or take action to correct the situation (Bonhoeffer, 2003).	The offense symbolically elevates the offender and diminishes the aggrieved (Loszak, 2014). Might exact revenge to re-establish levels (Akin, Ozdevecioglu, & Unlu, 2012). Might give grace, which correlates significantly with trait forgiveness and trait kindness (McConnell & Dixon, 2012; Palanski, 2012).	Grace is seen as a favorable attribute of leaders and organizations by some, but is often lacking in practice (Thomas & Rowland, 2014). Leaders might believe that demonstrating grace (e.g., compassion, kindness, empathy) will make them look weak but it actually causes them to be viewed as more genuine and trustworthy (Baldoni, 2023).
Giving/Receiving Grace		
Does not have an inherent right to receive grace (Corlett, 2013). When in receipt of grace compare it to 'being touched' with forgiveness, unconditional acceptance, love, help and connectedness (Schellekens et al., 2020). Received grace can result in liberation, new beginnings, and opportunities for personal growth (Schellekens et al., 2021). Upon receiving grace, is more likely to give grace to others (Schellekens et al., 2020) as their own trait self-forgiveness increases (Bufford et al., 2018)	Gives grace without requiring an apology (Garrard & McNaughton, 2003). Grace implies forgiveness: signaling unconditional acceptance and demonstrating benevolence (O'Connell, 2022) Giving of grace improves health outcomes for both parties (Costa & Neves, 2017; Lawler et al., 2005; Rasmussen, Stackhouse, Boon, Comstock, & Ross, 2019; Wallace, Exline, & Baumeister, 2008).	Can create cultures of grace and a climate of forgiveness to improve the well-being of employees and make the organization stronger and more resilient (O'Connell, 2022). In a culture of grace, employees benefit from improved job satisfaction, grace-giving, and reduced turnover intent (McConnell & Dixon, 2012, p.16).

Table 1: Key Concepts and Impacts on Stakeholders

grieved deciding whether or not to give grace, to forgive and/or to give mercy. The consequences of these decisions will have an impact, over time, on the offender, the aggrieved and the organization itself. To model this, we outline a stage model of grace giving.

Stage theories are triggered by a specific event (Siponen, 2024), in our case 'an offense' committed by an offender in the organizational context (Katz & Kahn, 1978). Pfarrer, Decelles, Smith, and Taylor (2008) suggest a four-stage model of recovery following an offense, comprising: (1) discovery, (2) explanation, (3) penance, and (4) rehabilitation. Gillespie and Dietz (2009) propose a four-stage model of trust repair after a transgression: (1) immediate response, (2) diagnosis, (3) reforming interventions, and (4) evaluation. Neither model includes contemplation of a decision to give grace, to forgive and/or extend mercy; in both cases, however, this is almost a given, as is penance in the first model. Neither model reflects the possibility that the offender may decide not to apologize, or that rehabilitation might be infeasible if forgiveness is not bestowed. Grace is not mentioned at all.

Enright (1996), however, proposes a staged forgiveness model, including four stages: (1) uncovering, (2) decision, (3) work, and (4) outcome. These stages help us to model the way our key concepts (apology, grace, forgiveness and mercy) come into play after an offense, and the role of grace as a game changer (Figure 3).

During the uncovering stage, the adverse incident occurs and the responsible offender may either accept responsibility, apologize, and show remorse or choose not to accept responsibility and not to apologize. The offender's choice during the uncovering stage is independent of whether grace will be bestowed by the aggrieved, or not.

Next, the aggrieved will decide whether to give grace or not. If the grace pathway is chosen, there is an inherent commitment to forgive and to show mercy. In contrast, if grace is not chosen by the aggrieved, they are choosing not to forgive. The work stage reflects the outcome of this choice. The aggrieved may still decide to show mercy, despite choosing the 'no grace' pathway. In these cases, they will not punish the offender.

Finally, the outcome stage highlights the consequences of the grace-related decision by the aggrieved. On the grace pathway, the offender learns from the incident and can engage in self-forgiveness, while the aggrieved reconciles with the offender. The organization thrives and flourishes as a consequence. On the other hand, if the grace pathway is not chosen, the offender may demonstrate defensiveness and rumination, while the aggrieved keeps score and estrangement may ensue. Conflict may manifest in such an organization. This, then, demonstrates the consequential and far-reaching power of grace in organizations.

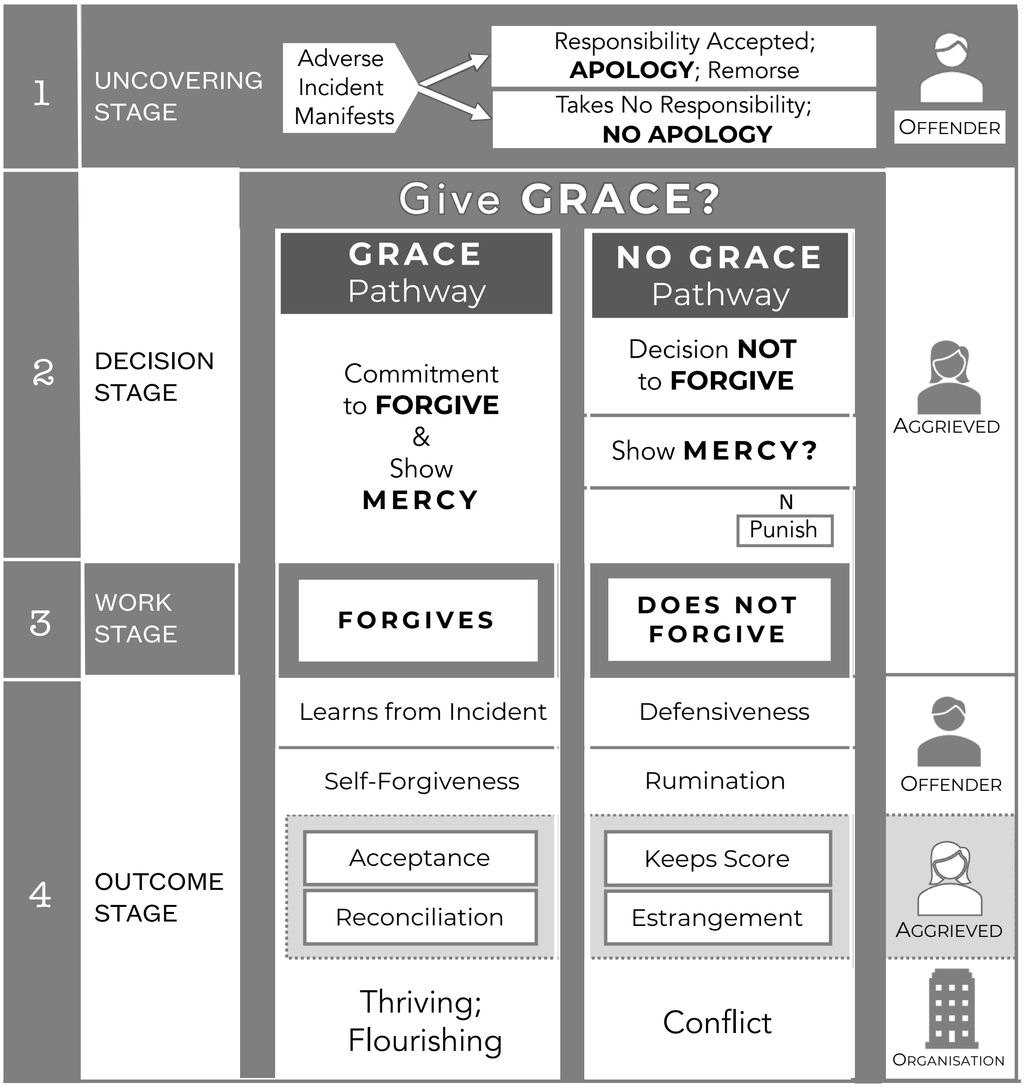

Figure 3: Offense Aftermaths with and without Grace

2.3 Emotion in Cybersecurity

Security demands can trigger an emotional overload (D'Arcy, Herath, & Shoss, 2014; D'Arcy, Herath, Yim, Nam, & Rao, 2018). This might explain why a general negativity towards cybersecurity has been observed (Renaud, Zimmermann, Schürmann, & Böhm, 2021; von Preuschen, Schuhmacher, & Zimmermann, 2024), specifically anger, fear, and annoyance (Fatoki, Shen, & Mora-Monge, 2024; Tian, Kanich, Polakis, & Patil, 2020) as well as being scared and confused (Haney & Lutters, 2018; von Preuschen, Zimmermann, & Schuhmacher, 2023). It seems that cybersecurity is a particularly apt context within which grace should manifest when things go wrong if the underlying current is already so negative and given that such negative emotions could reduce engagement with protective cybersecurity behaviors.

Offenses, in the context of cybersecurity, range from honest mistakes to deliberate abuses of organizational resources for illegal or malicious purposes.

In the *first* instance, an employee makes a cybersecurity mistake within an organization and forgiveness comes into play. An example is where they are deceived by a Phishing message, clicking on its link and allowing an external bad actor to gain access to the organization's systems (Fadilpašić, 2024). Another is an employee use of a public network which includes surveillance despite this site being forbidden by the organization (Jackson, 2024). Research is limited with respect to responses to these kinds of incidents. There is some suggestion that forgiveness should be granted (Taal, Le, & Sherer, 2016), but few empirical studies have considered the efficacy of such an approach in the cybersecurity domain.

In the *second* instance, an employee might deliberately use organizational resources to ill-intent (Chen, Guo, & Zeng, 2023; Eroglu, Peker, & Cengiz, 2022). Here, apologies could be tendered (Perez, 2021) but sometimes only when the offender is forced to do so (Nevett, 2023). There is no mention of forgiveness in these newspaper articles, nor whether grace came into play in the aggrieved's and organization's reactions to the offense.

Some researchers have explored emotions in response to adverse cybersecurity offenses. For example, Searle et al. (2024) outlines two pathways that could unfold in response to a cybersecurity incident which was mistakenly triggered by an employee. While these authors do not refer to forgiveness or grace, they do outline how, when employees are treated with understanding, the entire workforce can be reassured and the possible negative consequences of the incident on the workforce contained. They also highlight the likely negative outcomes, on multiple levels, when the offender is blamed, shamed and sanctioned for their mistake. They contend that the organization cannot flourish in this latter case.

It is challenging to find real-life examples of cases where employees receive grace in the context of adverse cybersecurity incidents. Organizations tend to handle these situations in-house. The external manifestation is usually an official apology from the organization with internal processes kept confidential. We could not find any mention of grace in these situations, nor of any research related to manifestations of grace in this context.

3 Study

We were primarily interested in situations where an employee (the offender) unintentionally triggered an adverse cybersecurity incident. Such an incident may suggest the need for an apology, remorse and a request for forgiveness from the aggrieved. Forgiveness may be understood, in part, as observable evidence of grace being manifesting in the situation (Bufford et al., 2017). We sought to answer the following research question: ***RQ:*** *To what extent might grace manifest in responses to adverse non-cybersecurity and cybersecurity incidents?*

3.1 Scenarios

Our focus was on gaining an understanding into how individuals respond to adverse non-cybersecurity and a cybersecurity incidents from multiple perspectives. By examining both kinds of incident, we were able to examine how responses to adverse cybersecurity incidents may be different from responses to non-cybersecurity incidents. Likewise, by having research participants consider multiple perspectives, we are able to obtain richer data and less biased data, as compared to only asking for an individual's own perspective (Yaniv & Choshen-Hillel, 2012).

We presented participants with two realistic (i.e., probable) scenarios in which one employee creates an adverse incident that disproportionately impacts another employee and probably the organization as a whole. Participants are then asked what they think may happen next and how the three primary entities involved (i.e., primary individual responsible for the adverse incident, a co-worker highly impacted by the incident, and management) may respond. We want to reveal what they think might occur during the 'Work Stage' in Figure 3 so that we can infer the activation of grace, or not. We expect them also to imagine what might occur during the 'Outcome Stage', which will help us to confirm whether the grace pathway was chosen, or not.

When they read the scenarios, participants had two choices: (1) attribute blame to, and potentially sanction, the individual, or (2) consider the context of the situation: the culture of the organization, environmental influences and other external contributors to the incident, leading to grace, mercy and forgiveness ('Decision Stage' in Figure 3). In the non-cybersecurity scenario, they could attribute blame to the individual for being deficient, lazy and derelict in letting down their team member. The other option is to consider that the organizational climate might well be toxic, the individual might have health issues or they might have been burnt out by a previous assignment. In the cybersecurity scenario, the individual may have failed to check the ‘from’ email address as they were trained to do, or simply have not cared enough and clicked without thinking. On the other hand, the Phishing message might have been so professionally crafted and well targeted that the person was genuinely taken in. In both cases, the participant chooses either to attribute the incident to the *individual* making it more likely that they will be sanctioned. They might, alternatively, consider surrounding influences that might have played a role, and suggest that these ought to be taken into consideration.

3.2 Quantitative Measures

In addition to the eight open-ended questions (four for each of the two scenarios), we also employed a series of instruments related to forgiveness and emotions for each of the scenarios. This was done to quantitatively assess their perceptions of forgiveness and other feelings for both scenarios. We did not specifically measure grace but rather its side effects, preferring to infer that grace came into play.

To assess how our participants thought the individuals in our scenarios might feel regarding forgiveness, we used the two-component motivational system related to avoidance (7-items) and revenge (5-items) — the ‘Transgression-Related Interpersonal Motivations (TRIM)’ scale (McCullough et al., 1998). Avoidance is associated with feelings of hurt, while revenge is related to righteous indignation feelings. We replaced the use of generic pronouns in the measurement items with the actual names of the individuals from the two scenarios to make it more salient for our participants. To reduce study fatigue while maintaining internal reliability, we reduced the number of items for each of the measures to three.

We also measured how our participants perceived the decision to forgive by the individuals in our scenarios by using three of the original five items from the ‘Decision to Forgive’ Scale (DTFS) (Davis et al., 2015). The goal of the DTFS is on measuring the decision to forgive as opposed to whether someone has reached the end state of forgiveness. And similar to our use of the TRIM, we modified the questions by replacing generic pronouns with the actual names of the individuals from our scenarios.

Trust in organizational settings inherently involves individuals being vulnerable to some degree. When adverse incidents occur, that trust may be violated with unintentional and often unpredictable consequences (Searle et al., 2024). Therefore, we also wanted to measure how willing our participants would be to engage in a series of behaviors with the individuals that caused the adverse incidents in both scenarios. The 'Behavioral Trust Inventory' (BTI) measures how vulnerable one is willing to be in work relationships (Gillespie, 2003). It is assessed through two sub-scales: 'reliance' and 'disclosure'. Reliance involves depending on the knowledge, actions, skills, or judgment of others. Disclosure may be described as information that is work-related and sensitive being shared with others.

Finally, we asked our participants to assess how the primary co-workers of the individuals in each scenario that caused the adverse incidents would feel given that it would in many respects disproportionately impact them. We used the the 'Positive Affect Negative Affect Schedule' (PANAS) (Watson, Clark, & Tellegen, 1988). The original PANAS consists of two independent 10-item scales, one for positive affect and one for negative affect. Positive affect is associated with how alert, enthusiastic, and active an individual demonstrates (Watson et al., 1988). In contrast, negative affect is associated with subjective distress, such as anger, disgust, and fear. As before, we reduced the number of items and instead of using 10 items for each construct, we used six.

3.3 Ethics

Prior to participant recruitment, Institutional Review Board approval was sought and obtained. This study qualified for exempt status given its minimal risk nature. In all cases, informed consent was obtained from research participants prior to participation. They were compensated with $20 for their time and effort, which takes into account recruitment and qualifying survey completion time.

3.4 Participant Recruitment

A pool of potential research participants were asked to complete a qualifying survey if they were interested in being considered for the current study. These individuals had participated in prior research studies a few years prior and were considered of much higher quality than what may often be found with crowd-sourced platforms, such as Amazon's Mechanical Turk. We received 123 completed responses to the qualifying survey. Of these, 91 were chosen to participate in the main study with a goal of achieving 60 valid responses.

The primary reason potential participants were excluded was because they were full-time students without any significant work experience to be able to reflect on the scenarios we would be presenting.

Prior to conducting large-scale data collection, a pilot study involving five participants was conducted. The data collected was evaluated by the research team to determine if there were any issues with the data, understanding of the questions, etc. No significant issues were identified. Therefore, the data from the pilot study was included as part of the complete data set.

Another 57 participants completed the main study. Two quality-control questions were employed in which the answers were obvious and on opposing ends of a Likert scale. Of 62 participants that started the survey before it was closed due to reaching our previously identified goal of 60 completed responses, two failed both quality control questions. None of the other participants failed a single quality control question. Likewise, nothing suspicious was identified during our qualitative analysis of the open-ended questions as has been noted elsewhere (Dupuis, Renaud, & Searle, 2022). Therefore, we had a total rejection rate of 3.2%. On average, it took participants approximately 30 minutes to complete the study.

3.5 Demographics

Our participants generally identified as female (71.7%), educated (68.3% had Bachelor's degree or higher), and their ethnicity as White (45%) or Asian (33.3%). Likewise, they tended to be younger (80% were between 20 and 39) and employed full-time (70%). While most of our participants did not supervise other employees (68.3%), many did as a regular part of their job (26.7%), and others did it part of the time (5%). Most individuals (61.7%) indicated that their current position did not involve cybersecurity responsibilities; however, some did indicate that their position involved such responsibilities part of the time (21.7%) or all of the time (16.7%).

4 Analysis & Results

The primary focus of our study and subsequent analysis was qualitative, which was the main factor in determining a sufficient sample size for analysis. While we also perform some quantitative analyses, we acknowledge that the sample size of 60 limits the available statistical power from which we may draw conclusions. However, it was sufficient to achieve saturation in the themes that emerged and particularly in the distinction between those arising in the non-cybersecurity and the cybersecurity adverse incident scenarios. Nonetheless, drawing on these combined analyses including our limited analysis from a quantitative perspective provides new insights and suggests potentially fruitful future research directions.

4.1 Qualitative Analysis

Our qualitative analysis leveraged the six-stage thematic analysis as outlined by Braun and Clarke (2006) including the following steps:

1. Becoming familiar with the data collected;
2. The generation of an initial set of codes;
3. Searching for themes from the coded data;
4. Theme refinement;
5. Define and further refine the themes;
6. Final analysis and report production.

Individually, the research team read through the data multiple times to become familiar with it prior to developing and assigning codes. This process was repeated for data from each of the two scenarios. Through this process, ideas, themes, and meaning began to emerge and an initial list of code candidates was developed (Braun & Clarke, 2006). Next, we went through the data and assigned codes for each entry to each open-ended question. We then used the codes assigned to the data to identify themes present within it. A large number of themes were identified at this stage, which was then refined in our fourth step. In examining the previously identified themes, we chose to eliminate, combine, separate, or keep them as is. This process was iterative in nature and was repeated until no additional substantive changes were needed. At that point, we defined and named the identified themes. Our goal was to fully outline the meaning of each theme. Our analysis from both scenarios follows.

In this section Pi denotes Participant number i.

4.1.1 Non-Cybersecurity Scenario

Responses to this scenario indicated that it had multi-level consequences including for the organization, as a whole, senior and line managers, as well as the two central individuals, Sam and Pat. Two distinct themes were evident in the responses. The **first** and most prevalent was one of blame and negative consequences especially for Sam; the **second** being future-focused directed towards understanding what had occurred and how to prevent it happening again.

The most common response centered on Sam, and the need to hold them accountable. There was a broad consensus that they should be reprimanded, with the majority of responses indicating they should be fired from the organization. Others included sanctions, demotion, retraining, or financial penalty. These incidents were considered to have tarnished their reputation, with efforts directed towards the need to restore and rebuild their lost trust. There was consensus that Sam's relationship with Pat and beyond (management) had been severely and possibly irrevocably damaged as the next quote exemplifies: "*Depending on the organizational structure and Pat and Sam's relationships with upper management, Sam would likely face some repercussions in addition to a strained relationship with Pat*" (P5). In reflecting on how these incidents could have been avoided, there was a consensus that Sam could have taken responsibility for what was unfurling and communicated more effectively and promptly with Pat; These efforts centered on tendering an apology, and asking for help. He/she could also actively engage in re-building trust, through two actions that could increase competence through additional training, or by directly asking a range of others how to make amends, as the next quote captures: "*Apologize, accept responsibility for the launch failure, discuss with leadership, ask how he can make it up*" (P10).

Participants either focused primarily on the dyad, regarding these incidents in relation to the two named actors, or the additional levels around them. As the previous quote identified, Pat had also been negatively impacted by the adverse incidents. Participants' responses distinguished the emotions that would follow these incidents and the range of future actions for Pat to undertake. All of the identified emotions were negative and ranged from 'upset' and 'disappointment', through to 'frustration', but far more typically the moral emotion 'anger'.

Most frequently suggested actions included: talking to Sam about what had occurred, raising concerns about Sam to management as a form of self-protection, through to blaming everything on Sam. Less common reactions were the ostracizing of Sam. the next quote captures a typical response: "*Pat and Sam could sit down together and discuss how they could have both worked better on coordinating smoothly*" (P23). Other future actions suggestions including not working again with Sam, for example "*Pat might be unhappy with Sam for being their downfall and might not want to work with him again*" (P26). It was also suggested it was important Pat put effort into restoring their own reputation as this incident had tainted both of them. For example, *"One or both of them may have faced handling less prestigious account until they could prove they were worthy of higher stakes again"* (P2).

Thus, without restoring trust, there could be further career consequences for both Sam and Pat. A few regarded these incidents as denoting a shortcoming from Pat and a likelihood of future consequences, as the next quote captures: *"Pat may also feel like her duties were not successful as she did not effectively manage his duties as a coordinator. They will most likely get written up, and have to go through some teamwork/group training to become better business partners"* (P29).

Responses to what Pat could do clearly recognized that, once burned, Pat might be wary of further interactions with Sam. While some reactions considered that trust would be damaged, others sought to use regular communication between the two to enable more positive collaborative working. Suggested actions included the merit of allowing Pat to articulate and acknowledge their feelings, while others involved their monitoring and record keeping about incidents. This latter suggestion was viewed as a means of self-protection to assure again for anything similar occurring in the future. However, respondents are clear Pat was not responsible, and therefore had limited options to to try and avoid such incidents from occurring as the following quotes indicates: *"Pat did everything they could in this situation by completing their work thoroughly. Perhaps maybe checking in with Sam about their work load and if they need help would be effective but I'm not sure what Pat could do"* (P27).

Managers were the next level identified in responses. This scenario was not neutral and tended to be negative but less extreme emotions were ascribed to managers than those indicated for Pat, including being 'upset'. A common action for managers was the value of talking either separately or together with Sam and Pat. Management efforts were primarily directed towards sanctions and punishment notably towards Sam, while a smaller set of responses focused on information gathering to understand what had gone wrong and to learn for the future. Managers were also involved in the allocation of future work, including subsequent workload allocations and the management of these now strained interpersonal relationships notably through avoiding putting these two employees together again. This suggestion is captured in the next quote: *"Pat and Sam will need to be called in individually to discuss where the project failed and why. Pat needs the opportunity to show his work and what had been done and Sam needs to show where he failed and why"* (P20). There was additional remedial work now required to ensure the ongoing monitoring of Sam (if they are not fired), and also with Pat to avoid future repetition, and specifically to re-assure Pat and restore their sense of justice, rather than risk impacting their ongoing engagement as the next quote indicates: *"Management could let Pat know that they recognized that they did their work and the loss was not entirely on Pat"* (P2).

Some respondents were more directive in the necessity of active trust repair efforts that attended to the emotional reactions but also restoring feelings of psychologically safe among their direct reports as the next quote indicates: *"Management could mediate the situation but they would have to ensure everyone feels safe. Management would need some serious trust building skills to help coach the team to get them back on track"* (P9). Further new work also was identified in the management of client relations. Thus these incidents had added further work to those at this level. For example: *"The team will have a retrospective and strategize how to fix the problem. If this doesn't get the project back on track, the leadership team will step in and fix the problem by pulling in new, higher performing folks"* (P9). It was clear from responses to the question about managers' responses to the incident that inaction was not an advisable, and instead a range of specific actions were required to help smooth relations, gather information and mitigate further adverse incidents.

The organization as a whole was noted as a consequence of individuals' actions specifically the loss of their current reputation, and potential future business losses. These reactions were far more limited. Finally, the client was the last level noted in some responses, and indicated the escalation of consequences outwith the organization and the dyad of Pat and Sam. Here, respondents noted the further actions now required to communicate and engage to mitigate further reputation loss. For some further reparations were also suggested in the form of financial sweeteners or reduced future terms.

In summary, responses to this scenario were clear about the source of the incident – Sam, and, to a limited extent, Pat. The key themes predominantly focused on the apportioning of blame and subsequent sanctions. A minority were more neutral, focusing on understanding and avoiding its future occurrence. Forgiveness was only mentioned twice in this scenario and only in relation to Pat: these included forgiving Sam, and more interestingly the following suggested actions that denotes forgiveness as part of a process for self-release: *"He needs to reflect on the situation, if there was something he could have done, find a way to improve and also forgive himself"* (P16).

Overall, the organizational context presents a unique dynamic for individuals with respect to their emotions and how they respond to incidents. The interplay of complex relationships of peers, subordinates, superiors, personal and organizational reputation, and dependencies (i.e., needing the paycheck), create a dynamic quite different compared to that which exists in the personal lives of individuals. Organizational culture may factor into this emotional interplay quite significantly, as well, and determine the extent to which grace, forgiveness, blame, etc., become the predominant outcomes, whether as emotions or virtues, in the aftermath of an organizational incident (Fehr & Gelfand, 2012). In the current scenario, the livelihood of one or more individuals is at stake, with several emotions at play, such as blame apportionment, trust repair, and overall negative emotions centered around strained organizational relationships. Beyond the limited mention of self-forgiveness, we see little here in our participants' responses to this scenario with regards to grace or forgiveness. The terms that are mentioned and reflected in our coding schema are indicative of negative emotions (e.g., hostility, guilt) (Watson et al., 1988) and are generally incompatible with grace or forgiveness.

4.1.2 Cybersecurity Scenario

Participants' responses to the cybersecurity scenario were distinct from those to the non-cybersecurity incident. Specifically, they were more reserved in their blaming and also more effective in demonstrating understanding and in coming up with ways to enable redemption and reconciliation for what ensued due to these incidents originating with a skilled external adversary as the following quotes indicated: *"I think most people would not question a mistake like this as it happens so easily given how savvy these phish scammers are"* (P20), and *"It's definitely a hard one though because sometimes these attempts are done so well that it could seem very real"* (P12). Thus, there was broad consensus that aside from getting someone else to check, there were limited ways to prevent such incidents, as the next quote captures in response to the question 'what could Alex have done?': *"Maybe asked for another set of eyes to double check if it was legitimate. Not much is to be done after a situation like this. It really doesn't seem like Alex did anything wrong if the hacking attempt was well crafted"* (P2).

In contrast to the previous scenario, this cybersecurity incident had three broad themes. **First**, these incidents triggered a speedy and established multi-level organizational process that comprised: (1) mass communication to all employees and potentially also clients, (2) the prioritizing of IT and management containment and repair efforts, (3) potential policy change, and (4) most frequently cited mandatory employee training to avoid further incidents. These processes can are designed to be restorative as the following quote illustrates, specifically by avoiding naming and punishing the individual: *"The issue will be resolved by the office teams. Leadership or Cybersecurity will issue a statement about what happened (without calling out Alex by name). All employees will receive additional training resources* *(mandatory completion) on how to watch out for cybersecurity threats. Everything will slowly go back to normal, and Alex should not face major repercussions for the accident"* (P14).

These organizational policies comprise formal mechanisms that are designed to support redemption and reconciliation, as the next quote reveals. However, these efforts aimed at restoring organizational-level trust through enhancing competence, can incur shared strong adverse reactions: "*Everyone takes cybersecurity training again and they all hate it*" (P3).

Managers, therefore, in contrast to the previous scenario, have a far more central role to play in the aftermath of cybersecurity incidents. Aside from their speedy implementation of the organization's cyber-security policies, they also have additional work to do to ensure these remain isolated incidents. As distinct from the other scenario, responses included the potential value of utilizing specific external experts to confirm either the veracity of the current response, or its further improvement. In addition to enhancing employees' cyber-detection skills, reactions could include technical solutions. There was consensus that rapid organization-wide reaction was necessary rather than a more *laissez-faire* or individual response as the next quote illustrates: "*Maybe management could have more security measures in place to not let scam emails through or ask themselves if Alex had all of their needs met in order to successfully complete the task. If they are overworked then maybe reducing their work load so they are able to make decisions with a fresh mind*" (P27).

Hence, management have to show that they have considered and attended to the underlying cause of these incidents. Further, responding to these adverse incidents can itself denigrate the resilience of their employee in the wake of an attack, requiring managers to anticipate and prevent further adverse consequences as the following quote captures: "*I think management should also step-in and work to help the employees maintain their work-life balance or reduce stress around the office while this issue is being dealt with. If employees have to stay late, maybe provide food or allow them to seek counseling with professionals to ensure that their mental health is okay*" (P37).

The **second theme** was focused on Alex. Here, there were two reactions: one focused on their formal reprimand with potential termination, and documentation of their error, with subsequent recognition and recognition policy implications, as the next quote indicates: "*Alex has a hard time getting a raise at their next review*" (P22). By contrast, a more frequent reaction was more understanding in the tone, and a focus on their trust restoration as the next quote shows: "*This is a mistake that even some people that have more experience may make, so I believe Alex would only need to be humble and accept that they've made a mistake,* *and own that*" (P28). Reactions revealed a broad consensus on this being achieved through a sequence commencing with an apology, undertaking further cybersecurity training, but also subsequent demonstrations of repentance, as the next quote outlines: "*Apologize and be willing to work harder than everyone else to rectify the situation*" (P5). Thus, there are clear further obligations required of these individuals by others in order to enable them to restore their former standing.

This greater understanding of respondents to cybersecurity incidents, however, was contingent on them not being repeated, enabling their actions to be attributed to 'human error' rather than a malicious intent. A typical example is found in the next quote: "*Own up to their mistake and apologize to the team. Make everyone know that they are aware of how the mistake occurred and will take careful consideration in the future to ensure there is not a repeat incident*" (P33). Indeed, participants' reactions revealed the futility of further sanctions through recognition of the internal consequences for victims as the next quote denotes: "*I don't think Alex should be punished because they are already facing enough negative consequences having to remedy the situation*" (P27). However, in place of organizational sanctions, a less obvious but no less impactful form of social sanction may be used by other employees to ostracize their colleague, as the next quote indicates: "*Alex may feel like an outcast and their coworkers might be extremely frustrated with Alex's action*" (P27). Similarly, Alex may feel the reduced trust or even distrust from superiors as the next quote captures: "*Management will trust him less and will have IT create stronger security protocols*" (P16). Therefore the resolution and role of forgiveness is a germane concern.

The **third and much smaller theme** concerned others' reactions, with far less attention on Jordan. There is a general consensus among respondents that Jordan has a limited role here. More clearly, however, there is a theme on the spillover to others of these incidents that is distinct to those in the non-cybersecurity scenario. These responses included some but less numerous negative emotions, with resentment the most apparent arising from the additional work Alex's error had created for them. Critically, far fewer emotions are mentioned in this cybersecurity scenario compared to the other, with less frequent selection of moral emotions such as anger, instead the reaction is more muted upset as the next quotes captures the dynamic stages following the incident comprising shared upset, then restorative action from Alex including their apology, learning, and additional work: "*I'm sure the whole office will be a bit upset with Alex about the incident, despite there being no malicious intent. I would hope that Alex would be apologetic about what happened and learn from her mistakes. Even with the apology, I'm sure it'd be upsetting to have to work more hours and put in all the extra* *work*" (P6).

Reflection on their actions, and the work the incident has created for others emerges as an important consideration for Alex. Aside from the apology, their efforts needs to be turned towards others to denote their new learning and the avoiding of subsequent incidents as the following quotes reveals: "*I think Alex needs to apologize to Jordan for the extra work. Maybe do something to help Jordan from getting burnt-out during this stressful time to show that they are taking their mistake seriously*" (P37). Importantly, others who work alongside the the individual responsible for cybersecurity incidents may be best placed to really identify whether these are indeed isolated incidents, or part of a wider pattern of risk taking. Therefore, while organizational policies may be designed to create the foundations of reconciliation and redemption, they may simply be too remote to have a more informed experience of these individuals' daily actions and whether they do warrant less understanding and indulgence.

Forgiveness is identified in the cybersecurity responses but it is sparse in the non-cybersecurity scenario. It centers on Jordan and their capacity to have empathy for another's errors and as a means of resolving their negative emotions (frustration) and allowing the significance of incidents to dissipate as the following quotes show: "*Maybe talk to Alex and vent his frustrations but also forgive so he could move on*" (P6), "*Jordan may try to recognize that anyone could have made this mistake and try to feel a bit more sympathy, grace, and forgiveness towards Alex.*" and "*Work on forgiveness and forgetting the situation*" (P14).

In contrast to the non-cybersecurity scenario, in which we see emotions emerge that are generally incompatible with grace and forgiveness, here, there are emotions and sentiments expressed that have brought us to the overarching concept of grace. The themes that emerged in this scenario from our participants relate to several different positive emotions and/or a reduction in negative emotions. For example, as blame has shifted and rationale provided for the incident, a clear reduction in negative emotions has occurred, including lower levels of anger, hostility, blameworthiness, disgust, etc. (Watson et al., 1988). Likewise, we see efforts to increase positive emotions, such as confidence, determination, attentiveness, concentration, alertness, etc. These expressions of generosity, mercy, and kindness by the participants toward Alex, regardless of whether Alex is deserving or not, is the very definition of grace that we provided earlier (Bufford et al., 2017). Thus, the unique context in which organizations exist and the relationships within them manifest may create unique opportunities for emotions to emerge commensurate with grace. In the current study, this occurred most notably in the context of a cybersecurity scenario, as opposed to a non-cybersecurity scenario.

Final themes are shown in Figures 4 and 5.

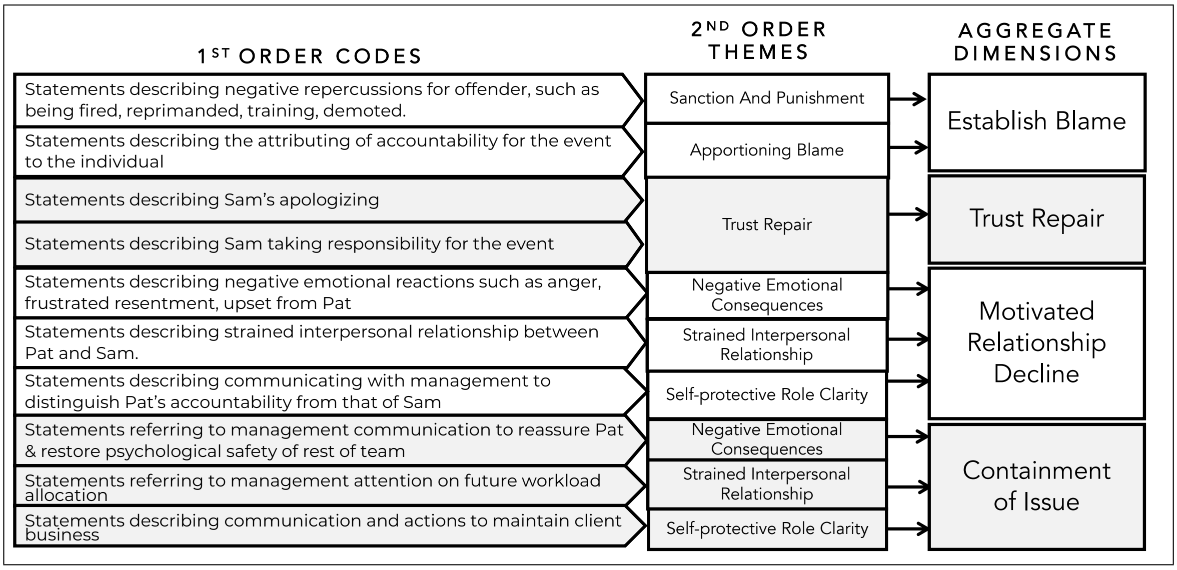
1ST ORDER CODES
2ND ORDER THEMES
AGGREGATE DIMENSIONS
Statements describing negative repercussions for offender, such as being fired, reprimanded, training, demoted.
Statements describing the attributing of accountability for the event to the individual
Statements describing Sam's apologizing
Statements describing Sam taking responsibility for the event
Statements describing negative emotional reactions such as anger, frustrated resentment, upset from Pat
Statements describing strained interpersonal relationship between Pat and Sam.
Statements describing communicating with management to distinguish Pat's accountability from that of Sam
Statements referring to management communication to reassure Pat & restore psychological safety of rest of team
Statements referring to management attention on future workload allocation
Statements describing communication and actions to maintain client business
Sanction And Punishment
Apportioning Blame
Trust Repair
Negative Emotional Consequences
Strained Interpersonal Relationship
Self-protective Role Clarity
Negative Emotional Consequences
Strained Interpersonal Relationship
Self-protective Role Clarity
Establish Blame
Trust Repair
Motivated Relationship Decline
Containment of Issue

Figure 4: Non-Cybersecurity Themes

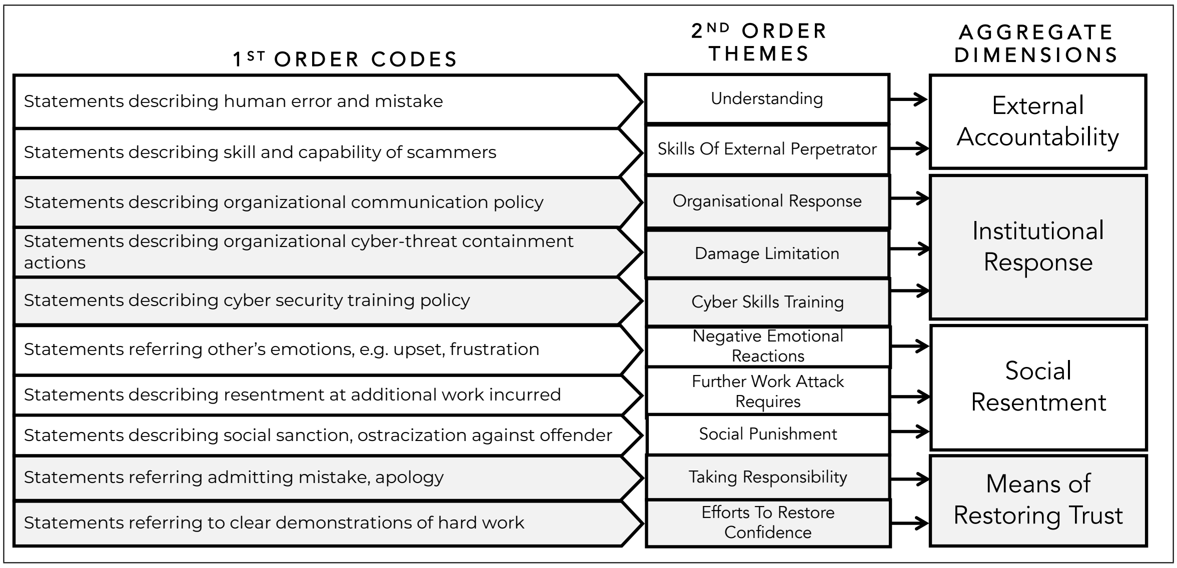
1ST ORDER CODES
2ND ORDER THEMES
AGGREGATE DIMENSIONS
Statements describing human error and mistake
Statements describing skill and capability of scammers
Statements describing organizational communication policy
Statements describing organizational cyber-threat containment actions
Statements describing cyber security training policy
Statements referring other's emotions, e.g. upset, frustration
Statements describing resentment at additional work incurred
Statements describing social sanction, ostracization against offender
Statements referring admitting mistake, apology
Statements referring to clear demonstrations of hard work
Understanding
Skills Of External Perpetrator
Organisational Response
Damage Limitation
Cyber Skills Training
Negative Emotional Reactions
Further Work Attack Requires
Social Punishment
Taking Responsibility
Efforts To Restore Confidence
External Accountability
Institutional Response
Social Resentment
Means of Restoring Trust

Figure 5: Cybersecurity Themes

4.2 Quantitative Analysis

The main focus of our quantitative analysis was on understanding the differences in how individuals viewed two significant adverse incidents for an organization based primarily on whether it was non-cybersecurity-related or cybersecurity-related. We began by assessing the reliability of the scales being used by calculating a Cronbach's Alpha value for each set. With only one exception (BTI-Non-Cybersecurity, Disclosure sub-scale), Cronbach's

Alpha was above .70. For this sub-scale, we removed one of the five items to improve our reliability to .716.

Next, we compared the results of our quantitative measures between the two adverse incident scenarios–non-cybersecurity and cybersecurity. In all instances, we conducted paired samples t-tests to support our statistical analyses.

The first instrument we used was the TRIM, which consisted of two sub-scales—avoidance and revenge. A paired samples t-test for avoidance showed how our participants, when assuming the role of Pat, the primary co-worker and individual impacted by Sam causing the adverse non-cybersecurity incident (M = 3.13, SD = 0.919), compared with the level of avoidance when they are Jordan, the primary co-worker and individual impacted by Alex in the adverse cybersecurity incident (M = 1.89, SD = 0.825; t = 9.69, $p < .001$, df = 59). Similar results are found for revenge in the adverse non-cybersecurity incident (M = 1.91, SD = .754) and adverse cybersecurity incident (M = 1.38, SD = 0.509; t = 6.27, $p < .001$, df = 59). Significantly higher levels of avoidance and somewhat higher levels of revenge were noted in the non-cybersecurity scenario as compared to the cybersecurity scenario, from the perspective of the primary co-workers.

Again, from the same perspective as the primary co-workers impacted by the adverse incidents, we assessed their decision to forgive the individual who caused the adverse incident by using the DTFS instrument. A paired samples t-test for decision to forgive showed how our participants (as Pat) in the adverse non-cybersecurity incident (M = 3.26, SD = 0.868), compared with the decision to forgive as Jordan, in the adverse cybersecurity incident (M = 4.01, SD = 0.720; t = -7.08, $p < .001$, df = 59). Our participants believed more strongly in the cybersecurity scenario than in the non-cybersecurity scenario that the primary co-worker should forgive the individual who caused the adverse incident.

Instead of having our participants assume the role of one of the individuals in the scenario, we had them indicate their willingness to engage in a series of behaviors with the individuals that had caused the adverse incidents. The two sub-scales of the Behavioral Trust Inventory (BTI) were measured—reliance and disclosure. A paired samples t-test for reliance in the adverse non-cybersecurity incident (M = 2.38, SD = 0.811), compared with reliance in the adverse cybersecurity incident (M = 4.26, SD = 1.26; t = -10.31, $p < .001$, df = 59). Likewise, the results for disclosure in the adverse non-cybersecurity incident (M = 3.26, SD = 1.147) and adverse cybersecurity incident (M = 4.32, SD = 1.470; t = -5.34, $p < .001$, df = 59) are significant and in a similar direction. Our participants indicated much higher levels of both reliance on, and willingness to, disclose sensitive information to Alex, the offending individual in the cybersecurity scenario, than Sam from the non-cybersecurity scenario.

Finally, we wanted to know how our participants thought these adverse incidents would make the primary co-worker feel by employing the two sub-scales of the PANAS, positive affect and negative affect. A paired samples t-test for positive affect showed how our participants, when assuming the role of Pat as the primary co-worker, were impacted by the adverse non-cybersecurity incident (M = 1.68, SD = 0.527), compared with the level of positive affect when they are Jordan, the primary co-worker impacted in the adverse cybersecurity incident (M = 1.517, SD = 0.483; t = 2.87, $p < .01$, df = 59). Similar differences are found for negative affect in the adverse non-cybersecurity incident (M = 3.45, SD = .747) and adverse cybersecurity incident (M = 3.08, SD = 0.836; t = 3.40, $p < .01$, df = 59). Interestingly, higher levels of both positive affect and negative affect are provided for the primary co-worker in the non-cybersecurity scenario when compared to the cybersecurity scenario with the mean difference higher in the latter than the former. The results of our quantitative analysis may be found in Table 2.

	M	**SD**	**t**	**p**	**df**
Avoidance			**9.69**	**p <.001**	**59**
Non-Cybersecurity	*3.13*	*0.919*			
Cybersecurity	*1.89*	*0.825*			
Revenge			**6.27**	**p <.001**	**59**
Non-Cybersecurity	*1.91*	*0.754*			
Cybersecurity	*1.38*	*0.509*			
Forgive			**-7.08**	**p <.001**	**59**
Non-Cybersecurity	*3.26*	*0.868*			
Cybersecurity	*4.01*	*0.720*			
Reliance			**-10.31**	**p <.001**	**59**
Non-Cybersecurity	*2.38*	*0.811*			
Cybersecurity	*4.26*	*1.26*			
Disclosure			**-5.34**	**p <.001**	**59**
Non-Cybersecurity	*3.26*	*1.147*			
Cybersecurity	*4.32*	*1.470*			
Positive Affect			**2.87**	**p <.01**	**59**
Non-Cybersecurity	1.68	0.527			
Cybersecurity	1.52	0.483			
Negative Affect			**3.40**	**p <.01**	**59**
Non-Cybersecurity	3.45	0.747			
Cybersecurity	3.08	0.836			

Table 2: Quantitative Results for Non-Cybersecurity vs. Cybersecurity Scenarios

5 Discussion

In this section, we discuss the key findings from our study in the context of the research question noted earlier. ***RQ:*** *To what extent might grace manifest in responses to adverse non-cybersecurity and cybersecurity incidents?*

5.1 Key Finding #1: Grace and Empathy

There was a contrast between reactions to the non-cybersecurity and the cybersecurity incident. Both our qualitative and quantitative analyses demonstrated condemnation and little tolerance towards the person who caused the non-cybersecurity incident, as opposed to greater empathy, compassion, grace and forgiveness in the wake of the cybersecurity scenario. The former triggered negativity towards the wrongdoer, with mentions of sanctions, demotions and job termination. There was a sense that the wrongdoer would be ostracized and would have to take deliberate steps to rebuild trust, including apologizing. They would have to 'make it up' to their team members, managers and the organization as a whole. The attribution was overwhelmingly individual: Sam messed up, Sam had to take accountability, and would be lucky to have a job the next day.

The cybersecurity scenario, on the other hand, elicited far more empathetic and non-blaming responses, i.e., grace. The empathetic response is not surprising as most individuals may have unwittingly fallen victim to a cybercrime at some point Norton (2021). According to Snow, "*...empathy can depend upon the empathizer's memories of having had experiences that are similar to what the other is undergoing*" (Snow, 2000, p.67). These shared experiences, often found in cybersecurity, create an environment conducive to empathy that may not be found in other contexts as illustrated in the non-cybersecurity scenario. When empathy is employed in the wake of a cybersecurity incident, it has the potential to transform what is often an adversarial dynamic to one that creates a more resilient organization Potter (2024). A predictor of empathy is grace, which is consistent with the role grace had in our cybersecurity scenario Hodge et al. (2022).

In the cybersecurity scenario, the attribution was often external: Alex might have been overworked, burnt out, or simply deceived by a well-crafted and convincing Phishing message. There was a sense that Alex ought to be supported rather than punished. There was mention of an organizational response, which we did not see in the non-cybersecurity incident, but which is common post-cybersecurity incidents: telling everyone what happened, remove the infection from the computers, retrain all staff to prevent re-occurrence. What is interesting here is that a similar study published in 2021 (Renaud, Searle, & Dupuis, 2021) revealed widespread condemnation of people whose mistake triggered an adverse cybersecurity incident. Some years later, people seem to have softened in their condemnatory stance, perhaps as a consequence of the prevalence of AI-powered attacks, which are increasingly difficult to spot (Renaud, Warkentin, & Westerman, 2023).

5.2 Key Finding #2: Non-Cybersecurity vs. Cybersecurity Scenarios

The use of two scenarios in this study was important primarily due to the differences between non-cybersecurity and cybersecurity incidents. The role of cybersecurity in an organization and the associated expectations placed on employees is entirely different from other responsibilities attached to a job role and, as such, a comparison between similar 'incident' scenarios is warranted.

Cybersecurity is an abstract concept for most employees that remains difficult to conceptualize in many respects (West, 2008). As an abstract concept, it can be difficult for an employee to understand and appreciate what is meant by some of the terminology or what risks are actually manifesting from a cybersecurity perspective. There is little that is abstract about the visuals or messaging needed for the average marketing campaign.

Additionally, very few individuals have job roles directly related to cybersecurity. Instead, it serves as a secondary task that, at best, acts as a road block to performing their primary tasks (Sasse, Brostoff, & Weirich, 2001; West, 2008). For these individuals, there is generally little expectation that they are experts in cybersecurity. In contrast, in our non-cybersecurity scenario the individuals involved are expected to be professionals (i.e., experts) at performing the assigned tasks (e.g., coordinating the creative team, visual and messaging alignment with the client's brand and objectives). The performance of most every other role by an employee other than cybersecurity is their *de facto* primary task. Emotional responses and performance expectations involving non-cybersecurity, as compared to cybersecurity situations, may also be different and is worth exploring.

Finally, organizations often approach cybersecurity for their employees in an adversarial manner—the organization versus the employee. In reality, it is generally the organization against the external threat (e.g., malicious hacker, malware). Largely as a function of the first two factors delineated in the preceding paragraphs, employees are generally ill-equipped to combat these external threats, instead being treated as if *they* were the threat

(Vidyaraman, Chandrasekaran, & Upadhyaya, 2007). Outside of cybersecurity, employees generally can be held accountable in a fair manner for their inability to perform their job tasks to a satisfactory level, as noted in the non-cybersecurity scenario. However, the same is seldom the case for incidents involving cybersecurity, as noted by many of our participants. Supporting a comparison between these two different types of scenarios was important to elucidate how such differences may manifest with respect to emotional responses and expectations. In the current study, this revealed a general feeling that more grace should be bestowed upon individuals caught up in cybersecurity incidents within their organization.

In Summary: The term 'forgiveness' was seldom mentioned by our participants. What *did* emerge from responses to the cybersecurity scenario was a growing realization that anyone could be deceived by a Phishing email, and that punishment in this case was unfair and unproductive – there was a sense that grace manifested in responses to this scenario. Participants were willing to consider external factors that could have led the offender to be deceived by a Phishing message whereas the non-cybersecurity lapse was attributed to the individual in question — no external attribution sprang to our participants' minds in this case.

Instead of explicitly mentioning forgiveness, much of the focus seemed to be related to empathy and comprehension — that this could happen to anyone. As such, the employees, management, and the organization should give grace to the individual who triggered the adverse cybersecurity incident.

Related to this is the different role cybersecurity often plays in an organization. Employees are generally focused on their primary task, which is usually not cybersecurity. Yet, they are tasked with cybersecurity responsibilities that are often far outside their area of expertise. In contrast, the non-cybersecurity scenario focused on tasks that were the primary tasks of the employee. Thus, the expectation of performing the tasks at hand competently is inherently different between the two scenarios.

This discussion does not take other kinds of cybersecurity incidents into account that could perhaps be far more damaging to the organization. Likewise, it also does not take the willingness of management to create a 'grace culture' into account or what exactly that may look like. However, it does reveal that there is a growing recognition of the inherent unfairness of cybersecurity sanctions on the average employee simply trying to do their job.

5.3 Practical Implications

Earlier, we discussed grace 'as a virtue'. While grace is indeed a virtue, it is not relegated to religious bodies and institutions alone as is so often assumed with virtues: it also exists beyond the realm of religion. It finds its way into all facets of our everyday lives, including within organizations where it may be viewed as a favorable attribute of both leaders and the organization itself (Thomas & Rowland, 2014).

Our participants generally believed grace was called for in response to the cybersecurity scenario. Most employees are not cybersecurity experts and most anyone can be tricked into clicking on a phishing email or otherwise fall victim to a cybersecurity scam. Thus, this implies issues around justice if harsh sanctions are employed against such employees. Instead, grace should be considered. When grace is shown in an organizational setting, especially in this context, it creates a more resilient and stronger organization that improves the well-being of its employees (O'Connell, 2022). Relationships are improved and there is an overall reduction in anxiety that allows employees to focus on what managers, executives, and shareholders want them to be most focused on—performing their job to the best of their ability (Deming, 1985).

When such focus exists, with employees performing at their best, they are also achieving the objectives of the organization at a much higher level, increasing the bottom line, and benefiting from an environment in which open communication is encouraged. Instead of employees being fearful of reprisal when a cybersecurity incident *does* occur, they know that the organization views the external attacker as the adversary rather than those within the organization simply trying to do their best. Ultimately, they know they are in it together, even when mistakes are made. When those mistakes *are* made, they will feel more comfortable informing the right personnel within the organization so the matter may be addressed promptly rather than a fearful employee hoping it will go away if they say nothing.

This shift in organizational culture is unlikely to occur overnight, but its benefits are worth pursuing (Fehr & Gelfand, 2012). While organizations have the option of holding onto traditional methods of accountability and punishment, some consideration should be given to a change in course in this regard, especially as it relates to cybersecurity. There will always be exceptions (e.g., malicious insiders); such exceptions should not dictate the rules that will make for stronger employees and organizations. Prior changes in how organizations operate, including from a quality control standpoint, have often been met with resistance but subsequently thrived (Maguad, 2006). The same can be true for creating a culture of grace. Given the numerous potential benefits to employees and the organization itself, it should be given due consideration.

5.4 Limitations

This study was based on the interpretation of two different scenarios from research participants rather than an examination of real-life case studies or an experimental manipulation in an actual organizational setting. While valuable insights may be gleaned from such scenarios, there are inherent limits to their generalizability. For example, we do not know the extent to which our research participants' views reflect how actual individuals would feel, respond, and react to such real-world situations.

Moreover, we collected self-reported qualitative and quantitative data from participants using a survey. And while multiple research methods were used, the risk of common method bias does remain a concern (Podsakoff, MacKenzie, Lee, & Podsakoff, 2003). This may be a function of factors such as the use of similar scale items, satisficing by respondents (i.e., social desirability bias), and providing data at a similar time, place, and format, among other factors. The fact that the surveys did not have the participants' names associated with their responses and that they were self-reported rather than administered by a researcher help mitigate social desirability bias to some extent (Nederhof, 1985). Nonetheless, such concerns cannot be completely eliminated.

Our sample was skewed towards female respondents. This could have meant a greater tendency to forgiveness than if the sample had been more gender balanced (Miller, Worthington Jr, & McDaniel, 2008). However, this tendency, if it played a role in responses, would likely have had an equal impact across both scenarios, and would not explain the greater grace extended to the offender in the cybersecurity context.

6 Conclusion & Future Work

In this paper, we sought to investigate grace using two realistic scenarios. We presented the scenarios to 60 participants with four open-ended questions for each, as well as multiple instruments to assess their perceptions, feelings, and attitudes related to the individuals in the scenarios and from their own perspective as well.

When an individual makes a mistake, others may assume that all responsibility for that mistake rests with the individual. However, this is short-sighted and often neglects the context within which incidents occur. This is true for cybersecurity mistakes in organizational settings as well. Organizations can foster a culture of grace to ensure that this pathway is likely to become a conscious and default choice when managing the aftermath of adverse incidents.

In criminology, transformative justice seeks to help all entities in the wake of wrongdoing, including the community at large (Ruttenberg, 2022). If those involved are merely restored to their state prior to the wrongdoing, it is likely that the conditions that caused the incident in the first place will cause a re-occurrence. However, if we acknowledge and recognize how intertwined all facets of the organization are, including policies, culture, context, etc., then we may be able to effectuate positive change that significantly limits future mistakes. This will more effectively serve all individuals and the organization at large, both in the short- and long-term.

Many of our participants noted the need for improvements in processes to address the adverse incidents described in the two scenarios — transformative justice. It was never just about blaming the individual, especially in the case of the cybersecurity scenario. There is an inherent recognition among our participants that cybersecurity is not the primary task for most employees (West, 2008). Instead, cybersecurity generally serves as a secondary task that is abstract in nature and gets in the way of end users performing their primary task.

A culture of grace can be present before and after an adverse incident. It is not dependent on something going wrong, but is instead a philosophy: proactive rather than reactive. As noted earlier, it has many benefits, including removing fear and creating a more positive and supportive work environment. It is good for the long term health of the organization and the well being of its employees. Nonetheless, we also acknowledge that grace may have unintended consequences if not properly managed. For example, when an employee receives grace in the wake of a violation it may seem unfair to co-workers (O'Connell, 2022). The challenge lies in balancing grace with concepts such as obligation, accountability and reciprocity, which might be incompatible with the concept of grace in some circumstances. In these cases, grace could perhaps mitigate sanctions and permit the offender to restore the situation and their own reputation.

The current study examined how our participants responded to scenarios which reflected the aftermath of adverse incidents detailed in two organizational scenarios. Grace and changes in processes emerged as prevailing themes, especially in response to the cybersecurity scenario. To the extent that some organizations implement such approaches, are they effective in an cybersecurity context? What does an effective implementation consist of? These questions could be explored further with an emphasis on balancing the cybersecurity needs of an organization, while also providing a culture of forgiveness and grace. As noted earlier, organizations with such cultures benefit both the organization and its employees.

Acknowledgments

We will make our anonymized data available via the Open Science Foundation should this paper be accepted.

References

Akhtar, S. (2002). Forgiveness: Origins, dynamics, psychopathology, and technical relevance. *The Psychoanalytic Quarterly*, *71*(2), 175–212. (https://doi.org/10.1002/j.2167-4086.2002.tb00010.x)

Akin, M., Ozdevecioglu, M., & Unlu, O. (2012). The relationship between revenge intention and forgiveness tendency with mental health of employees in organizations. *Amme Idaresi Dergisi*, *45*(1), 77–97.

Baldoni, J. (2023). Leading with grace when the pressure is on. *Leader to Leader*, *2023*(108), 37–42. (https://doi.org/10.1002/ltl.20704)

Beautement, A., Sasse, M. A., & Wonham, M. (2008). The compliance budget: managing security behaviour in organisations. In *Proceedings of the 2008 new security paradigms workshop* (pp. 47–58). (https://doi.org/10.1145/1595676.159568)

Bonhoeffer, D. (2003). *Discipleship: Dietrich Bonhoeffer Works, vol. 4.* Minneapolis: Fortress Press.

Brady, D. L., Saldanha, M. F., & Barclay, L. J. (2023). Conceptualizing forgiveness: A review and path forward. *Journal of Organizational Behavior*, *44*(2), 261–296. (https://doi.org/10.1002/job.2632)

Braun, V., & Clarke, V. (2006, January). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101. (https://doi.org/10.1191/1478088706qp063oa)

Brudholm, T. (2020). Apology without forgiveness. *Social Research: An International Quarterly*, *87*(4), 835–861. (https://dx.doi.org/10.1353/sor.2020.0066)

Bufford, R. K., McMinn, M. R., Moody, J. A., & Geczy-Haskins, L. (2018). The effects of grace interventions in church communities. *The Journal of Positive Psychology*, *13*(5), 512–521. (https://doi.org/10.1080/17439760.2017.1350740)

Bufford, R. K., Sisemore, T. A., & Blackburn, A. M. (2017). Dimensions of grace: Factor analysis of three grace scales. *Psychology of Religion and Spirituality*, *9*(1), 56. (http://dx.doi.org/10.1037/rel0000064)

Chen, Z., Guo, W., & Zeng, Q. (2023). Factors Influencing Social Media Forgiveness Behavior and Cyber Violence Tendency Among Chinese Youth: Moderating Effects of Forgiveness Climate and Risk Perception. In J. Abdelnour Nocera, M. Kristín Lárusdóttir, H. Petrie, A. Piccinno, & M. Winckler (Eds.), *IFIP Conference on Human-Computer Interaction* (p. 449–468). York, UK: Springer. (https://doi.org/10.1007/978-3-031-42286-7_25)

Corlett, J. A. (2013). *Responsibility and punishment* (Vol. 34). Dordrecht: Springer Netherlands. (https://doi.org/10.1007/978-94-007-0776-4)

Corlett, J. A., & Corlett, J. A. (2004). Forgiveness, mercy, and retributivism. *Responsibility and Punishment: Revised Second Edition*, 98–112.

Costa, S. P., & Neves, P. (2017). Forgiving is good for health and performance: How forgiveness helps individuals cope with the psychological contract breach. *Journal of Vocational Behavior*, *100*, 124–136. (https://doi.org/10.1016/j.jvb.2017.03.005)

Cram, W. A., Proudfoot, J. G., & D'Arcy, J. (2021). When enough is enough: Investigating the antecedents and consequences of information security fatigue. *Information Systems Journal*, *31*(4), 521–549. (https://doi.org/10.1111/isj.12319)

D'Arcy, J., Herath, T., & Shoss, M. K. (2014). Understanding employee responses to stressful information security requirements: A coping perspective. *Journal of Management Information Systems*, *31*(2), 285–318. (https://doi.org/10.2753/MIS0742-1222310210)

D'Arcy, J., Herath, T., Yim, M.-S., Nam, K., & Rao, H. R. (2018). Employee moral disengagement in response to stressful information security requirements: a methodological replication of a coping-based model. *AIS Transactions on Replication Research*, *4*(1), 8.

Davis, D. E., Hook, J. N., Van Tongeren, D. R., DeBlaere, C., Rice, K. G., & Worthington, E. L. (2015). Making a decision to forgive. *Journal of Counseling Psychology*, *62*(2), 280–288. (https://doi.org/10.1037/cou0000054)

Deming, W. E. (1985). Transformation of Western Style of Management. *Interfaces*, *15*(3), 6–11.

Dupuis, M., Jennings, A., & Renaud, K. (2021, October). Scaring people is not enough: An examination of fear appeals within the context of promoting good password hygiene. In *Proceedings of the 22st annual conference on information technology education* (p. 35–40). SnowBird UT USA: ACM. Retrieved from `https://dl.acm.org/doi/10.1145/3450329.3476862` doi: 10.1145/3450329.3476862

Dupuis, M., Renaud, K., & Jennings, A. (2022, January). Fear might motivate secure password choices in the short term, but at what cost? In *Proceedings of the 55th hawaii international conference on system sciences (hicss) 2022* (p. 4796–4805). Virtual. Retrieved from `https://scholarspace.manoa.hawaii.edu/handle/10125/79922` doi: 10.24251/HICSS.2022.585

Dupuis, M., Renaud, K., & Searle, R. (2022, September). Crowdsourcing Quality Concerns: An Examination of Amazon's Mechanical Turk. In R. Trygstad & P. Zheng (Eds.), *The 23rd Annual Conference on Information Technology Education* (p. 127–129). Chicago IL USA: ACM. (`https://doi.org/10.1145/3537674.3555783`)

Emmons, R. A., Hill, P. C., Barrett, J. L., & Kapic, K. M. (2017). Psychological and theological reflections on grace and its relevance for science and practice. *Psychology of Religion and Spirituality*, *9*(3), 276. (`http://dx.doi.org/10.1037/rel0000136`)

Enright, R. D. (1996, Jan). Counseling within the forgiveness triad: On forgiving, receiving forgiveness, and self-forgiveness. *Counseling and Values*, *40*(2), 107–126. (`https://doi.org/10.1002/j.2161-007X.1996.tb00844.x`)

Eroglu, Y., Peker, A., & Cengiz, S. (2022, November). Cyber victimization and well-being in adolescents: The sequential mediation role of forgiveness and coping with cyberbullying. *Frontiers in Psychology*, *13*, 819049. (`https://doi.org/10.3389/fpsyg.2022.819049`)

Fadilpašić, S. (2024). *The FIA has been hacked after workers fell for a phishing attack.* (`https://www.techradar.com/pro/security/the-fia-has-been-hacked-after-workersfell-for-a-phishing-attack`)

Fatoki, J. G., Shen, Z., & Mora-Monge, C. A. (2024). Optimism amid risk: How non-it employees' beliefs affect cybersecurity behavior. *Computers & Security*, *141*, 103812. (`https://doi.org/10.1016/j.cose.2024.103812`)

Fehr, R., & Gelfand, M. J. (2010). When apologies work: How matching apology components to victims' self-construals facilitates forgiveness. *Organizational Behav-*

ior and Human Decision Processes, *113*(1), 37–50. (https://doi.org/10.1016/j.obhdp.2010.04.002)

Fehr, R., & Gelfand, M. J. (2012). The forgiving organization: A multilevel model of forgiveness at work. *Academy of Management Review*, *37*(4), 664–688. (https://doi.org/10.5465/amr.2010.0497)

Garrard, E., & McNaughton, D. (2003). III-In defence of unconditional forgiveness. *Proceedings of the Aristotelian Society (Hardback)*, *103*, 39-60. (https://doi.org/10.1111/j.0066-7372.2003.00063.x)

Gillespie, N. (2003). *Measuring trust in working relationships: The behavioral trust inventory*. Melbourne Business School. (https://www.econbiz.de/Record/measuring-trust-in-working-relationships-the-behavioral-trust-inventory-gillespie/10001769936)

Gillespie, N., & Dietz, G. (2009). Trust repair after an organization-level failure. *Academy of Management Review*, *34*(1), 127–145. (https://doi.org/10.5465/amr.2009.35713319)

Haney, J. M., & Lutters, W. G. (2018). " it's {Scary… It's}{Confusing… It's} dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)* (pp. 411–425).

Hodge, A. S., Hook, J. N., Davis, D. E., Van Tongeren, D. R., Bufford, R. K., Bassett, R. L., & McMinn, M. R. (2022, May). Experiencing grace: A review of the empirical literature. *The Journal of Positive Psychology*, *17*(3), 375–388. (https://doi.org/10.1080/17439760.2020.1858943)

Hoffman, K. D. (2008). Forgiveness without Apology: Defending Unconditional Forgiveness. In *Proceedings of the American Catholic Philosophical Association* (Vol. 82, pp. 135–151). (https://doi.org/10.5840/acpaproc20088210)

Jackson, J. (2024). *Germany spills British military secrets to Russia.* (https://www.telegraph.co.uk/world-news/2024/03/03/germany-intelligence-leak-uk-troops-ground-ukraine-nato/)

Katz, D., & Kahn, R. L. (1978). *The social psychology of organizations* (2nd ed.). New York, USA: John Wiley & Sons.

Kleine, A.-K., Rudolph, C. W., & Zacher, H. (2019). Thriving at work: A meta-analysis. *Journal of Organizational Behavior*, *40*(9-10), 973–999. (https://doi.org/10.1002/job.2375)

La Caze, M. (2006). The asymmetry between apology and forgiveness. *Contemporary Politi-*

cal Theory, *5*, 447–468. (https://doi.org/10.1057/palgrave.cpt.9300259)

Lawler, K. A., Younger, J. W., Piferi, R. L., Jobe, R. L., Edmondson, K. A., & Jones, W. H. (2005). The unique effects of forgiveness on health: An exploration of pathways. *Journal of Behavioral Medicine*, *28*, 157–167. (https://doi.org/10.1007/s10865-005-3665-2)

Lawler-Row, K. A., Scott, C. A., Raines, R. L., Edlis-Matityahou, M., & Moore, E. W. (2007). The varieties of forgiveness experience: Working toward a comprehensive definition of forgiveness. *Journal of Religion and Health*, *46*, 233–248. (https://doi.org/10.1007/s10943-006-9077-y)

Lewicki, R. J., Polin, B., & Lount Jr, R. B. (2016). An exploration of the structure of effective apologies. *Negotiation and Conflict Management Research*, *9*(2), 177–196. (https://doi.org/10.1111/ncmr.12073)

Loszak, K. (2014). Failing with grace. In B. Willock, R. C. Curtis, & L. C. Bohm (Eds.), *Understanding and Coping With Failure* (p. 15-22). Routledge.

Maguad, B. A. (2006, March). The modern quality movement: Origins, development and trends. *Total Quality Management & Business Excellence*, *17*(2), 179–203. (10.1080/14783360500450608)

McConnell, J. M., & Dixon, D. N. (2012). Perceived forgiveness from God and self-forgiveness. *Journal of Psychology and Christianity*, *31*(1), 31. (https://doi.org/10.1080/17439760.2024.2314293)

McCullough, M. E., Rachal, K. C., Sandage, S. J., Worthington Jr, E. L., Brown, S. W., & Hight, T. L. (1998). Interpersonal forgiving in close relationships: Ii. theoretical elaboration and measurement. *Journal of Personality and Social Psychology*, *75*(6), 1586–1603. (https://doi.org/10.1037/0022-3514.75.6.1586)

Miller, A. J., Worthington Jr, E. L., & McDaniel, M. A. (2008). Gender and forgiveness: A meta–analytic review and research agenda. *Journal of Social and Clinical Psychology*, *27*(8), 843–876. (https://doi.org/10.1521/jscp.2008.27.8.843)

Murphy, J. G. (2006). Remorse, apology, and mercy. *Ohio St. J. Crim. L.*, *4*, 423.

Nederhof, A. J. (1985). Methods of coping with social desirability bias: A review. *European Journal of Social Psychology*, *15*(3), 263–280. (https://doi.org/10.1002/ejsp.2420150303)

Nevett, J. (2023). *Gavin Williamson ordered to apologise over bullying texts to Wendy Morton.* (https://www.bbc.com/news/uk-politics-66706287)

Norton. (2021). *2021 Norton Cyber Safety Insights Reports Global Results*. Retrieved from https://us.norton.com/content/dam/norton/pdfs/reports/2021_nortonLifelock_cyber_safety_insights_report_global_results.pdf

O'Connell, D. (2022). Grace in the workplace: A process model of its impact. *Journal of Management, Spirituality & Religion*, *19*(4), 364–389. (https://doi.org/10.51327/OAKX1041)

O'Connell, D., & Adams, M. (2024). Measuring the dynamics of grace at work. *The Journal of Positive Psychology*, 1–18. (https://doi.org/10.1080/17439760.2024.2314293)

Ong, M. (2023). The transforming power of self-forgiveness in the aftermath of wrongdoing. *Organizational Behavior and Human Decision Processes*, *176*, 104237. (https://doi.org/10.1016/j.obhdp.2023.104237)

Palanski, M. E. (2012). Forgiveness and reconciliation in the workplace: A multi-level perspective and research agenda. *Journal of Business Ethics*, *109*, 275–287. (https://doi.org/10.1007/s10551-011-1125-1)

Perez, L. (2021). *Chrissy Teigen Issues Apology Following Cyberbullying Controversy: "How Could I Have Done That?".* (https://www.hollywoodreporter.com/news/general-news/chrissy-teigen-issues-apology-cyberbullying-1234967598/)

Pfarrer, M. D., Decelles, K. A., Smith, K. G., & Taylor, M. S. (2008). After the fall: Reintegrating the corrupt organization. *Academy of Management Review*, *33*(3), 730–749. (https://doi.org/10.5465/amr.2008.32465757)

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. (https://doi.org/10.1037/0021-9010.88.5.879)

Potter, L. (2024). Towards an anthro-centric cybersecurity. In M. Artz & L. Koycheva (Eds.), *EmTech Anthropology* (p. 64–81). Routledge.

Rasmussen, K. R., Stackhouse, M., Boon, S. D., Comstock, K., & Ross, R. (2019, May). Meta-analytic connections between forgiveness and health: the moderating effects of forgiveness-related distinctions. *Psychology & Health*, *34*(5), 515–534. (https://doi.org/10.1080/08870446.2018.1545906)

Reason, J. (1995). A systems approach to organizational error. *Ergonomics*, *38*(8), 1708–1721. (https://doi.org/10.1080/00140139508925221)

Renaud, K., & Dupuis, M. (2019). Cyber security fear appeals: Unexpectedly complicated.

In *Proceedings of the New Security Paradigms Workshop* (p. 42-56). Costa Rica: ACM. (https://doi.org/10.1145/3368860.3368864)

Renaud, K., Dupuis, M., & Searle, R. (2022). Cybersecurity Regrets: I've had a few .... *Je Ne Regrette*. In *Proceedings of the New Security Paradigms Workshop* (p. 1–20). New Hampshire, USA: ACM. (https://doi.org/10.1145/3584318.3584319)

Renaud, K., Searle, R., & Dupuis, M. (2021). Shame in cyber security: effective behavior modification tool or counterproductive foil? In *New Security Paradigms Workshop* (p. 70–87). Online: ACM. (https://doi.org/10.1145/3498891.3498896)

Renaud, K., Warkentin, M., & Westerman, G. (2023). From ChatGPT to HackGPT: Meeting the cybersecurity threat of generative AI. *MIT Sloan Management Review*.

Renaud, K., Zimmermann, V., Schürmann, T., & Böhm, C. (2021). Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, *8*(1), 1–17. (https://doi.org/10.1057/s41599-021-00746-5)

Rutigliano, N. K. H., Barkevich, S., & Hurley, B. (2017). Forgiveness in the Workplace: Fuel for Individual and Organizational Success. In *Encyclopedia of Strategic Leadership and Management* (p. 877-–889). Hershey, USA: IGI Global. (https://doi.org/10.4018/978-1-5225-1049-9.ch061)

Ruttenberg, D. (2022). *On repentance and repair: making amends in an unapologetic world*. Boston: Beacon Press.

Sasse, M. A., Brostoff, S., & Weirich, D. (2001). Transforming the 'weakest link'-a human/computer interaction approach to usable and effective security. *BT Technology Journal*, *19*(3), 122–31.

Schellekens, T., Dillen, A., Dewitte, L., & Dezutter, J. (2021). A lay definition of grace: A quantitative and qualitative content analysis. *The International Journal for the Psychology of Religion*, *31*(2), 79–101. (https://doi.org/10.1080/10508619.2020.1793593)

Schellekens, T., Dillen, A., & Dezutter, J. (2020). Experiencing grace: A thematic network analysis of person-level narratives. *Open Theology*, *6*(1), 360–373. (https://doi.org/10.1515/opth-2020-0108)

Schneider, C. D. (2000). What it means to be sorry: The power of apology in mediation. *Mediation Quarterly*, *17*(3), 265–280. (https://doi.org/10.1002/crq.3900170305)

Searle, R., Renaud, K., & van der Werff, L. (2024). Shaken to the core: Trust trajectories in the aftermaths of adverse cyber events. *Journal of Intellectual Capital*. (In Press)

Siponen, M. (2024). Stage theorizing in behavioral information systems security research. In *Hawaii International Conference on System Sciences.* Honolulu, 3-6 January. (`https://hdl.handle.net/10125/106952`)

Snow, N. E. (2000). Empathy. *American Philosophical Quarterly*, *37*(1), 65–78.

Taal, A., Le, J., & Sherer, J. (2016). Increased C-suite recognition of insider threats through modern technological and strategic mechanisms. In R. Koch & G. Rodosek (Eds.), *European Conference on Cyber Warfare and Security* (p. 428-434). Munich: Academic Conferences International Limited.

The Hindu Newspaper. (2005). *Descent of divine grace.* (`https://web.archive.org/web/20060512000536/http://www.hindu.com/2005/06/30/stories/2005063000400900.htm`)

Thomas, M., & Rowland, C. (2014). Leadership, pragmatism and grace: A review. *Journal of Business Ethics*, *123*, 99–111. (`https://doi.org/10.1007/s10551-013-1802-3`)

Tian, H., Kanich, C., Polakis, J., & Patil, S. (2020). Tech pains: characterizations of lived cybersecurity experiences. In *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)* (pp. 250–259). (`10.1109/EuroSPW51379.2020.00040`)

Vidyaraman, S., Chandrasekaran, M., & Upadhyaya, S. (2007). Position: The user is the enemy. In *New Security Paradigms Workshop* (p. 75–80). North Conway, NH: ACM. (`https://doi.org/10.1145/1600176.160018`)

von Preuschen, A., Schuhmacher, M. C., & Zimmermann, V. (2024). Beyond fear and frustration-towards a holistic understanding of emotions in cybersecurity. In *Twentieth Symposium on Usable Privacy and Security (SOUPS 2024)* (pp. 623–642).

von Preuschen, A., Zimmermann, V., & Schuhmacher, M. C. (2023). How do you feel about cybersecurity? - a literature review on emotions in cybersecurity. In *International Symposium on Technikpsychologie (TecPsy) 2023* (pp. 1–13). (`https://doi.org/10.3929/ethz-b-000619643`)

Wallace, H. M., Exline, J. J., & Baumeister, R. F. (2008, March). Interpersonal consequences of forgiveness: Does forgiveness deter or encourage repeat offenses? *Journal of Experimental Social Psychology*, *44*(2), 453–460. (`https://doi.org/10.1016/j.jesp.2007.02.012`)

Watson, D., Clark, L. A., & Tellegen, A. (1988, June). Development and Validation of Brief Measures of Positive and Negative Affect: The PANAS Scales. *Journal of Personality* *and Social Psychology*, *54*(6), 1063–1070. (https://doi.org/10.1037/0022-3514.54.6.1063)

West, R. (2008). The psychology of security. *Communications of the ACM*, *51*(4), 34–40. (http://doi.acm.org/10.1145/1330311.1330320)

Yaniv, I., & Choshen-Hillel, S. (2012). When guessing what another person would say is better than giving your own opinion: Using perspective-taking to improve advice-taking. *Journal of Experimental Social Psychology*, *48*(5), 1022–1028. (https://doi.org/10.1016/j.jesp.2012.03.016)

Zheng, X., Van Dijke, M., Leunissen, J. M., Giurge, L. M., & De Cremer, D. (2016). When saying sorry may not help: Transgressor power moderates the effect of an apology on forgiveness in the workplace. *Human Relations*, *69*(6), 1387–1418. (https://doi.org/10.1177/0018726715611236)

A Non-Cybersecurity Scenario

Please read the following scenario:

Pat and Sam work as project managers in a bustling marketing firm. Their current project involves launching a new advertising campaign for a major client. The deadline is tight, and the stakes are high as the client expects nothing short of perfection.

Pat is responsible for coordinating with the creative team, ensuring that the campaign's visuals and messaging align with the client's brand and objectives. Sam, on the other hand, is tasked with managing the budget, liaising with vendors, and ensuring timely delivery of materials.

As the deadline approaches, Pat diligently oversees the creative process, providing feedback, and making sure everything is on track.

However, Sam falls behind on managing the budget and fails to secure necessary resources within the allocated funds.

Despite Pat's efforts to keep the project moving smoothly, the campaign hits a roadblock when key vendors refuse to deliver without full payment. With crucial elements missing, the campaign launch is delayed, causing frustration for both the client and the internal team.

The delay tarnishes the firm's reputation, leading to financial losses and strained client relationships. Pat and Sam face repercussions for the failure.

1. What do you think might happen next?
   What would it take to help Pat to feel more positive after their last experience?

2. Is there anything Sam would have had to have done in the interim to achieve this? Please specify what.

3. Is there anything Management would have had to have done in the interim to achieve this? Please specify what.

4. Is there anything Pat would have had to have done in the interim to achieve this? Please specify what.

B Cybersecurity Scenario

Please read the following scenario:

Alex and Jordan work together as administrative assistants in a bustling office environment, handling various tasks to keep the office running smoothly. Despite their non-technical roles, they both understand the importance of cybersecurity protocols and receive regular training on how to identify and avoid potential threats.

One busy morning, Alex receives an email appearing to be from a reputable vendor the company frequently works with, requesting urgent confirmation of a recent order. The email contains a link labeled ″Review Order Details.″ Without pausing to scrutinize the email closely, Alex clicks on the link, assuming it's a routine request related to their work.

Unbeknownst to Alex, the email is a well-crafted phishing attempt designed to trick recipients into revealing sensitive information or downloading malicious software. By clicking on the link, Alex inadvertently triggers a malware download that infects the office's network, compromising sensitive data and disrupting essential systems.

As the malware spreads through the network, it causes chaos in the office. Files become corrupted, email accounts are compromised, and critical systems grind to a halt. Alex and Jordan, along with their colleagues, are thrust into crisis mode, scrambling to contain the damage and restore normal operations.

The incident results in significant negative outcomes for everyone involved. The office experiences a loss of productivity as employees struggle to complete tasks without access to essential tools and resources. The IT department is overwhelmed with the task of identifying and mitigating the security breach, while management faces pressure to address the fallout and prevent future incidents.

Alex feels a profound sense of guilt and anxiety over their role in the cybersecurity incident. Both Alex and Jordan, along with their colleagues, must work overtime to rectify the situation, exacerbating their stress and impacting their work-life balance.

1. What do you think might happen next?
   What would it take to help Jordan to feel more positive after their last experience?

2. Is there anything Alex would have had to have done in the interim to achieve this? Please specify what.

3. Is there anything Management would have had to have done in the interim to achieve this? Please specify what.

4. Is there anything Jordan would have had to have done in the interim to achieve this? Please specify what.