Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?

Karen Renaud
University of Strathclyde, UK
Rhodes University, RSA
University of South Africa, RSA
karen.renaud@strath.ac.uk

Rosalind Searle
University of Glasgow
Glasgow, UK
rosalind.searle@glasgow.ac.uk

Marc Dupuis
University of Washington
Bothell, USA
marcjd@uw.edu

ABSTRACT

Organizations often respond to cyber security breaches by blaming and shaming the employees who were involved. There is an intuitive natural justice to using such strategies in the belief that the need to avoid repeated shaming occurrences will encourage them to exercise more care. However, psychology highlights significant short- and long-term impacts and harmful consequences of felt shame. To explore and investigate this in the cyber domain, we asked those who had inadvertently triggered an adverse cyber security incident to tell us about their responses and to recount the emotions they experienced when this occurred. We also examined the impact of the organization's management of the incident on the "culprit's" future behaviors and attitudes. We discovered that those who had caused a cyber security incident often felt guilt and shame, and their employers' responses either exacerbated or ameliorated these negative emotions. In the case of the former, there were enduring unfavorable consequences, both in terms of employee well-being and damaged relationships. We conclude with a set of recommendations for employers, in terms of responding to adverse cyber security incidents. The aim is to ensure that negative emotions, such as shame, do not make the incident much more damaging than it needs to be.

CCS CONCEPTS

• **Security and privacy** → **Social aspects of security and privacy**; Usability in security and privacy; • **Applied computing** → **Psychology**; **Sociology**.

KEYWORDS

Shame, guilt, cyber security incident, responses, consequences

ACM Reference Format:
Karen Renaud, Rosalind Searle, and Marc Dupuis. 2021. Shame in Cyber Security: Effective Behavior Modification Tool or Counterproductive Foil?. In *New Security Paradigms Workshop (NSPW '21), October 2021, New Hampshire, USA.* ACM, New York, NY, USA, 17 pages. https://doi.org/000

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from permissions@acm.org.
NSPW '21, October 2021, New Hampshire, USA
© 2021 Association for Computing Machinery.
ACM ISBN 000…$15.00
https://doi.org/000

1 INTRODUCTION

Falling victim to a scam can induce long-term trauma [140]. The considerable distress that follows the realisation of having been duped into something, such as handing over lifelong savings, can transform into ignominy during the inevitable follow-up with the associated financial institution. Such investigations often feel like interrogations rather than restorative actions, seeming primarily focused on absolving the institution of any blame [24]. Strikingly, cyber crime is the only area of misdemeanor where the victim is often deemed to be culpable [146].

In the organization context, cyber security professionals often regard the human user as "a problem to be solved", meaning that they develop and impose interventions designed to constrain, control and thereby 'save' their organizations from their employees' propensities to compromise cyber security [160]. Organizations ensure that employees are aware of organizational security policies. These efforts highlight the negative consequences of breaches, often employing threats of sanctions against those who do not comply [109]. It is understandable that organizations who fear cyber security incidents elect to utilize 'fear appeals' to encourage compliance [113] in an attempt to scare employees into behaving securely. When an employee causes an adverse cyber security event, the organization's response, regardless of whether any malice was intended, tends to be punitive [14]. A recent survey of organizations found that 42% punish their employees for cyber security incidents [63]. Helpnet revealed that 15% name and shame employees, 33% decrease access privileges, 63% inform the employee's line manager and 17% lock them out of their computer until remedial re-training is completed.

These actions position shame as a resource: a means to 'civilise' employees [117, p.1], broadcasting the adverse consequences of non-compliance. Shamers co-opt shame as an organizational tool, rather than acknowledging that these emotions hurt individuals. Wong and Tsai [152, p. 209] quote Mencius, a Chinese Philosopher, who says: "*Men cannot live without shame. A sense of shame is the beginning of integrity.*" Yet, a contrary perspective contends that behaviours are determined less by negative emotions such as shame and guilt, and more by positive emotions including truth, justice and fairness [91]. The act of shaming might serve only to make the shamer feel superior, achieving very little behavioural change in the shamed [28].

Organizational applications of shame are expanding, extending into new domains, including cyber security. However, given the complexity of emotions such as shame and guilt [141], we need to contemplate its use, and more critically consider its subsequent long-term impacts, as a precursor to its wider embrace. Our exploratory

study of organizational reactions to non-malicious lapses focuses on qualitative retrospective insights into adverse cyber security events to consider the advisability of shaming in the cyber security domain.

This paper makes three contributions. *First*, we advance insights into moral emotions, specifically the self-condemning emotion of shame, increasing understanding of its propensities and its efficacy in encouraging future compliance with organizational policies. *Second*, we review the reported utilisation of shame in cyber security related research. *Third*, we demonstrate conceptually, and confirm empirically, how the consequences of applying shame could easily "go awry" (using Tangney *et al.*'s phraseology [137]).

We reveal how shaming can paradoxically make organizations *less* secure, with the elicitation of shame leading to avoidance and withdrawal behaviours and hiding of future mistakes [54]. Thus, instead of the anticipated 'civilisation' of employees, it is likely that the organization's risk *rises* with the use of shame. We contend that shaming is unlikely to be the efficacious behaviour modification tool many believe it to be, and instead outline how such applications are liable to backfire, causing more harm than good.

Section 2 commences with an exploration of shame and its dimensions, to distinguish it from its close cousin, guilt. Section 3 then considers shame's applications in the cyber security domain. Section 4 poses the research questions and survey instrument. Section 5 reports the findings, Section 6 discusses and reflects on these, offering recommendations based on the findings, and acknowledging the study's limitations. Section 7 concludes.

2 THE NATURE OF SELF-CONSCIOUS EMOTIONS

Shame and guilt are both negative self-conscious emotions, evoked by self-reflection and self-evaluation [136, p.347]. Both can cause intrapsychic pain [136] as well as physiological responses [39, 55]. The human brain evaluates everything in terms of potential threat or benefit: rational thought follows this initial intuition [57]. This means that negative emotions have a fundamental and pervasive influence on the way we respond to events in our everyday lives. That being so, both guilt and shame in a work context are likely to impact our future relationships with our colleagues and careers.

Guilt and shame are widely, but not universally, acknowledged to be substantively different emotions [23]. Jaffe *et al.* [66] analyzed different languages, and discovered that all make sharp distinctions between these emotions, but that there did not seem to be any adaptive advantage to either.

To understand shame, we need first to understand the dimensions of both guilt and shame: their similarities and differences.

2.1 Shame and Guilt Dimensions

Sadeghen [122] cites Higgins [64] who provides a way to distinguish between these emotions. He explains that the self can be separated into three elements: (1) the *actual* self - who you are, (2) the *ideal* self - who you think you should be, and (3) the *ought* self - who you wish you could be. Guilt, according to Higgins, occurs when there is an inconsistency between the 'actual self' and the 'ought self', whereas shame is an inconsistency between the 'actual self' and the 'ideal self'. Tracy and Robins [141] point to this incongruence as being precursor to the occurrence of the emotions of guilt and shame.

Teroni and Deonna [139], in their differentiation between shame and guilt, also argue that shame is linked with *ideals*, aligning with Higgins' characterization.

In contrast, Brookes [23] considers guilt to be a particular kind of shame. He argues that the person who has committed a wrong act subsequently *feels* guilt. Hence, he does not believe that the act can be separated from the person who committed it, which appears to negate the idea that guilt and shame are distinctly different emotions. He argues that shame is part of a type of super-set, with guilt being just one kind of shame, related to wrongful actions that we can apologize for. He does concur that guilt offers a path to redemption, whereas shame does not always offer a way to expiate. He contends that the kind of shame that is *not* guilt is characterized by the person *not* accepting responsibility for the harm they have caused. This chimes with Wang's [147] assertion that the shamed find it difficult to apologize. In concluding, Brookes argues that 'guilt' is simply shame that can be relieved by moral repair and is related to minor wrongdoing.

Whereas most of the authors we cite in this paper consider both shame and guilt to be emotions, Elison [44] argues that a person can be guilty without emotion; that it is actually an external and objective phenomenon. However, when someone reflects on their guilt and then *feels* bad about it, or is fearful of the consequences, an emotion is triggered. Hence Elison argues that we should compare shame with "feelings of guilt" in order to be strictly accurate. To save space, we shall use 'guilt' to refer to these feelings for the rest of the paper.

Kasabova's [73] perspective on shame is that it is embedded when there is an opposition between emotion (disgrace and loss of face) and morals (virtue) where it has implications between self-worth and social disapproval, which also aligns with Higgins' characterization. This leads us neatly into the first difference: the focus of each emotion.

Focus of the Emotion: Lewis [84] differentiates between the two by whether the trigger of this emotion is either 'the person', or 'the wrong act'. He argues that the former triggers shame, while the latter results in guilt. Confirmation for this distinction is found in Agarwal and Duhachek [3] who concur that shame focuses on the *individual* as the perpetrator of the wrong action, whereas guilt points to the consequences for 'others' of the wrong action. Trevino *et al.* [142] also support this view.

A different perspective is outlined by Carolsson [27] who argues that shame is invoked when the wrong act is *attributed* to a particular person, making them morally responsible for it. Guilt, on the other hand, is related to making a person *accountable* for a particular act. She uses two different words in this respect. In holding people accountable, they are considered to *deserve* guilt, but when responsibility is attributed, it is *fitting* for them to feel shame. This is a distinct focus on either the action (deserving) or the person (fitting).

In particular, guilt and shame emotions have very different impacts on individuals, and on the idiosyncratic responses they produce [135]. Tangney and Dearing [135, p.31] explain that feelings of guilt arise from "*some failure or violation of moral standards.*"

Lewis outlines that shame is "*a painful emotion that arises when one appraises a threat to the self of falling short of an important standard tied to one's identity*" [85] (cited by [34, p.2449]).

In summary, the final outcome of a negative self-experienced emotion can be shame, if attribution is global (i.e. the person) [141], or guilt if the attribution is related to a specific behavior (i.e. action) [108]. Critically, the latter opens the way to reparation and apology, while the former hurts the person's vulnerable self-hood.

Shame as a social construct: Sznycer *et al.* [134] explain that shame has evolved as a defense against devaluation, confirming Daniels *et al.*'s [34] argument that it is always socially constructed. Zahavi explains that shame "*affects and alters our relationship to and connectedness with others*" [157, p.223]. Kasabova [73] quotes Aristotle [7] as arguing that people feel shame before those whose opinion matters to them.

Garvey [49] offers a further distinction, suggesting that shaming someone invokes a sense that other people's eyes are on the shamed person, judging and condemning them. Imposing a sense of guilt, on the other hand, focuses attention on the wrongful action, and on the ways that the person could try and repair the situation. Therefore, it does not necessarily affect their social standing. Wenzel *et al.* [148] shows how defensiveness increases in response to social/moral threat. Defensive actions are a typical self-preservation response, and considered to be unlikely to lead to productive outcomes, either in the short- or long-term.

A critical aspect of shame is that it arises as a consequence of being devalued by peers. Therefore, something that peers consider wrong is necessary for someone to feel shame. Hence, it is not about doing wrong *per se*, rather it is knowing that others perceive shortcomings in one's moral character due to having taken an action that peers **believe is wrong regardless of whether or not it is actually wrong**. As a consequence feelings of shame stir [116], even if the action was not a moral failing.

This makes its application by organizations to achieve behavior modification particularly insidious. An employee could do wrong but fail to perceive any ramification in how others see them. Indeed, social and cultural variance in perceptions of morality can result in wide deviations in the situations and events that elicit shame and the possibility of reparation is also influential [54]. Imposing shame by means of exclusion can influence the employee's choice of restorative actions based on whether they consider resolution to be feasible. Instead of focusing on a consequence of wrongdoing, shame seems almost to shift into the realms of mind-control rather than morality.

Shame- and Guilt-Related Pain: A further distinction between these two arises from differences in the internal suffering produced. Shame is associated with *personal* devaluation. Through this devaluation, a person's self-identity is affected, producing feelings of self-condemnation. There is a sense that guilt is less painful because the guilty are able to make reparation and also because the pain is associated with the *act* and not with the person [50, 56, 58]. Tangney *et al.* [135] agrees that shame is more painful, and can lead to a shrinking of self, and accompanying feelings of worthlessness and powerlessness. This is echoed by Plate [106, p.82], who explains that someone experiencing shame feels 'faulty, worthless or wrong'.

Scheff [123] refers to shame as the 's-word', claiming it to be taboo in our 21st century lives. It is often hidden, and impacts on people's lives in the form of withdrawal, violence and conflict with others. Echoing this sentiment, Pivetti *et al.* [105] contends that shame makes people feel like a failure. Middelton-Moz argues that people are ashamed of their shame [93, p. xi]. Taylor [138] calls shame the "nitroglycerine of emotions"

Many scholars have written about the particular painfulness of shame [27, 53, 124, 136]. Tomkins *et al.* [79, p. 133] states that shame is felt "*as an inner torment, a sickness of the soul*", with Kirchner *et al.* [76] concurring it is 'unbearably painful'. Jung regarded shame as *" a soul-eating emotion"* [70, p. 232], arguing that people will do a great deal to try and avoid it. While this reaction might seem desirable, Gilbert points out that: "*Prestige seeking and shame avoidance can lead to some very destructive behaviours indeed*" [52, p.1225].

Individual/Cultural Differences: Tangney *et al.* [136] contend people are either shame-prone, or guilt-prone. The former, they suggest, are likely to experience shame in response to some form of personal failure, or error. In a consumer-based study, Sinha and Mandel [129] found that an individual's high risk tolerance rendered shame appeals powerless.

Other studies reveal significant cultural and individual differences in how people respond to shame [17, 65, 76]. For example, Kobayashi *et al.* [78] found that the perceived threat of shame would lead Japanese workers to comply with institutional rules more than American workers. Bagozzi *et al.* [10] reported that Dutch workers considered shame to threaten their self-esteem, and responded by reducing their performance. In contrast, Filipino workers perceived shame as a threat to their social status, and so responded in the opposite way by improving their performance.

The differences between guilt and shame drawn out during this section are summarised in Table 1.

Table 1: Different dimensions of shame and guilt

Shame	**Guilt**
Painful. Self-conscious. Caused by event that is incongruent with identity goals	
Discrepancy between *actual* self and *ideal* self	Discrepancy between *actual* self and *ought* self
Focused on person	Focused on behavior
Individual shortcoming attribution	Behavior-specific appraisal
Self protective response likely	Reparation response likely
Destructive long-term consequences	Constructive long-term consequences
Internal affective state	External objective state
Ideals	Prohibitions
Outcome=hubris	Outcome=regret
Avoidance tendency	Approach tendency
Negative behavioral responses in future	Wiser future decisions

2.2 The Shame Process

A further way that shame has been explored is in terms of a process, comprising distinct stages [108]:

2.2.1 *Trigger:*

Lewis [85] identifies three kinds of behaviors that trigger shame. These include: moral transgressions, performance failures, or a violation of social norms. In order for shame to arise, Reason [111] explains that the individual needs to appraise their behavior and view it as departing from their own behavioral standards, which are tied to their identity. This deviation is attributed to their actions, and thus arises due to internal and stable causes. Drawing on social cognitive theory [12], this creates a negative, but also global, moral assessment, and so shame occurs [136]. Similarly, where such transgression contravenes accepted social norms, shame will arise, with the individual motivated to try and hide their activities in an effort to avoid social sanction [12].

In much the same way as fear appeals are used, 'shame appeals' can also attempt to prompt *anticipatory shame*. In this case, various intensities of shame can be induced. Tracy and Robins [141] highlight the difficulties of eliciting specific self-conscious emotions, unlike more basic emotions such as joy and fear. Marketing studies have found that including the words 'guilt' or 'shame' in an advert can activate these emotions in viewers [41]. However, these can be rather blunt tools, which do not allow for the tailoring of the intensity of the desired emotional response. As a consequence, they are imprecise and unpredictable in their impact.

Boudewyns *et al.* [19] suggest that medium shame intensity has the greatest chance of encouraging people to engage in a desired behavior. Studies indicate that low levels of elicited shame can explain the failures of interventions to lead to compliance [121]. This study was related to green advertisements in Finland, and both the application and country context are likely to have influenced the outcome.

In contrast, higher intensity shame experiences make people more likely to engage in self-protective responses [83]. However, they found an exception where extremely high shame intensity was experienced, causing the shamed person to acquiesce and engage in the desired restorative responses, such as apologising. Ahmed *et al.* [4] warn that when the shame emotion is too strong, the consequence could be a *reduction* in future compliance.

These results indicate the difficulty in achieving an optimal level of shame intensity, because self-protective responses do not simply depend on shame intensity. Instead, self-esteem [13, 153] and the person's culture (individualistic or collectivist) [10] can also play a role.

2.2.2 *Response:*

There is some evidence that guilt leads to more favourable and constructive responses, whereas shame is likely to lead to negative and destructive reactions [1, 30, 87, 102, 105, 136]. Tangney *et al.* [137] expands this view, in terms of:

Guilt → acceptance: this option is likely to lead to an apology and an attempt to make amends.

Shame → self protective responses: If people experience shame, they engage in a *cognitive review* of the shame-related experience and associated internal scripts. Those experiencing shame will try to restore their threatened self [36] to protect themselves from further harm [118]. Tangney enumerates a number of responses people could engage in as they do this: (1) attack themselves (e.g., self-disgust), (2) withdraw [83], (3) avoid [159], or (4) attack others (e.g., blame, aggression and anger [75, 144]), deterring further communication as a means to diminish shame-related distress [128].

Crossovers: People can indeed respond to shame with acceptance [98]. Leach and Cidam [81] suggest that shame can give rise to a reparative response *if there is a perception that the situation is indeed reparable* [41, 92]. Examples include apologising, the changing of future behaviors, attempts to explain what happened, and to punish oneself, after ruminating about what has occurred [22].

However, as Miller and Tangney [95] argue, this is much less likely. Those experiencing guilt or embarrassment are more likely to accept the emotion and be able to adapt and recover by engaging in restorative actions. These responses to shame reveal important and detrimental differences from guilt with individuals' responses ultimately not assisting them either to restore their damaged moral image, or to engage with change in their future actions. Instead, they try to step away and specifically avoid positive problem-based reflection [118]. Indeed, those who experience shame are less likely to apologize for their actions, and instead are more likely to attempt to hide their transgressions. The failure to engage in a reparative process makes individuals carry on with their behaviors, and intensify their future moral emotional burdens about the events triggered by these [147]. Indeed, Xi *et al.* [155] reported that shamed employees increased emotional exhaustion.

2.2.3 *Long-Term Consequences:*

Considering process, there are other impacts of shame that concern its physiological and psychological responses, with shame wounding the psyche and leaving more enduring scars. Monica Lewinsky, who was shamed in front of the world, said: "*shame sticks to you like tar*"[1]. Wright *et al.* [154] showed how shame could trigger depression, leading to anti-social and border personality disorders [59]. Similarly, Livne *et al.* [88] found that employees who respond to exploitation internally, notably through shame and guilt, were more likely to experience burnout, silence and withdrawal. Finally, Dickerson *et al.* [39] identified the psycho-biological changes shame can induce, increasing pro-inflammatory cytokine activity to produce negative health consequences.

Shame has been found to interfere in the quality of the relationship between leaders and followers (i.e., managers and those they supervise) [106]. This is particularly acute when it goes unacknowledged either by the person inflicting shame, or the one experiencing it. Therefore, it is unsurprising to find that the failure to constructively manage shame can, in the long run, result in unethical behaviors [97].

2.2.4 *Long-Term Behavioral Change:*

In terms of future behaviors, Tangney *et al.* [136] report that while guilt can be effective in motivating people to choose the right path, shame does not operate in the same way.

Zhuang [159] argues that guilt leads people to take greater care, changing their attitudes towards future risk, but that no similar

[1] https://www.theguardian.com/technology/2016/apr/16/monica-lewinsky-shame-sticks-like-tar-jon-ronson

attitudinal shifts are found for shame. For example, in examining alcohol consumption Dearing *et al.* [37] found the desired reduction was reported for those who felt guilt, but not when they felt shame.

In terms of helping people to avoid the same situations in the future, some researchers have investigated how counterfactual thinking can help [101]. Niedenthal *et al.* [101] found that counterfactual thinking enabled those who had experienced guilt to conceptualize different responses to similar events. In contrast, those experiencing shaming found counterfactual thinking much more difficult to achieve due to the global attribution of the fault. They contend that this is because the individual has to contemplate changes to their self, with all the rejection that implies. In essence, shame hurts when it happens, but also colours all future decisions negatively.

2.2.5 A Process Model of Shame:

Figure 1 offers a synthesis of the literature, developing a process model of shame, which demonstrates the complexity of the shame emotion and confirms the need to determine whether its use in an organizational context to achieve behavioral modification is indeed wise, or ill-advised.

2.3 Why Do Organizations Utilize Shame?

When an organization wants to persuade their employees to comply with procedures and processes, or to cease any unwanted behavior, they often use fear, retraining, naming and shaming [111]. This utilization of shame is highlighted by Creed *et al.* [40]. It is also used as a deterrent, as a means of retribution, but also for rehabilitation [49]. Reason [111] contends that such perspectives are predicated on a core belief: the "just world" hypothesis i.e. bad things happen to bad people. By implication, those who experience bad outcomes have moral failings which makes them deserve their punishment. In this way, he suggests "*blaming individuals is more satisfying than targeting institutions*" [111, p.770]. While the word 'institution' is used by Reason, for the purposes of this paper the word 'institution' is considered equivalent to 'organization'. It is also often a more convenient parsimonious means of constraining the perceived source of the 'problem' to an isolated deviant. This misses the opportunity to carry out a wider review of systems and contextual influences, which could reveal issues which remain to trip up other employees.

In an investigation of the use of 'self-conscious' emotions, including shame and guilt, from a social work context, Gibson [51] discovered that the threat of shame and promise of praise were used as mechanisms of institutional control. Through these means, the organization attempted to create employees' compliance through fostering institutionally 'acceptable' behaviors. As a result, he concludes that emotions are being used as a "technology of power", confirming the findings of others [5, 125].

2.4 Does Imposing Shame Work?

While guilt appeals *can* result in attitude change [156], there is some disagreement in the literature about whether shame can achieve the same level of behavioural change. Some report that shame is efficacious [3, 15, 41, 86, 92, 100], while others consider it to be counter-productive [19, 21, 102, 152].

Review of organizational studies reveal how both withdrawal and reparative responses from employees can be driven by shame [54]. Critically, the choice of response is based on whether restoration is regarded as possible [35], with more challenging or risky reparation likely to result in withdrawal. Because it threatens self-identity, shame can lead to beneficial outcomes, as individuals strive to regain a more positive self-image as good and helpful employees [18, 60].

It can also result in more obvious efforts to apologize and be seen to be more transparent and accommodating [10, 60]. Furthermore, in contexts of high interdependence, both the quality of relationships as well as organizational performance can be enhanced [10]. In contrast, where reparation is viewed as less likely or impossible, employees can avoid others and withdraw, reducing their efforts and performance as a consequence [145]. Responses to shame that arise from circumstances outwith individual control, such as from inability in a particular domain, can lead employees to try and hide their limitations [62], while if it stems from interpersonal conflict, uncooperative self-serving behaviors such as competition, neglect or avoidance, can escalate [16].

Notably, displays of shame can have an appeasing function, interpreted by others as indications of the individual's moral awareness and of their regret [90, 96]. Kador contends that, at its heart, an apology is an exchange of shame and power between two parties [71].

Garvey [49] dissects this question in his study of a criminal domain. He points out that while shame 'seems' intuitively to be a viable alternative to incarceration, it can also backfire very easily. He argues that shaming can push an offender into committing further offenses because of society's reaction to the shaming event. If a shamed person tries to protect her or himself from the pain imposed by the shame, this can lead to their no longer caring about the sanctions that their community imposes. In this way, they become immune to the social norms.

He also explores the idea of rehabilitation. He contends that when someone commits an action which leads someone in authority to use shame to bring them back into line, the availability of a reparative act is likely to make the difference to that person in terms of moving on. If they see the shame as a rejection of their personhood, then reparation is constrained with little way for them to continue to function as a fully-fledged member of that community. In this way, shaming can become a destructive force.

Sinh [100] tested the comparable impacts of guilt and shame appeals through an examination of health communication, to conclude that their effectiveness depends on context. Furthermore, Zuzelo [161] shows how by providing support, together with shame appeals, can produce a constructive response. This discussion emphasises Tangney *et al.*'s [137] warning about the ease with which shame can "go awry."

3 SHAME IN CYBER SECURITY RESEARCH & PRACTICE

Having reviewed the literature on shame, and the different stances taken with respect to its use in organizations, we now consider its use in cyber security. There are arguments both *for* [45, 69, 89, 94, 143] and *against* its use [107, 114] in the cyber security domain.

Confirmation of Shame Responses: Having to deal with a cyber security incident can produce negative emotions [110, 115, 149,

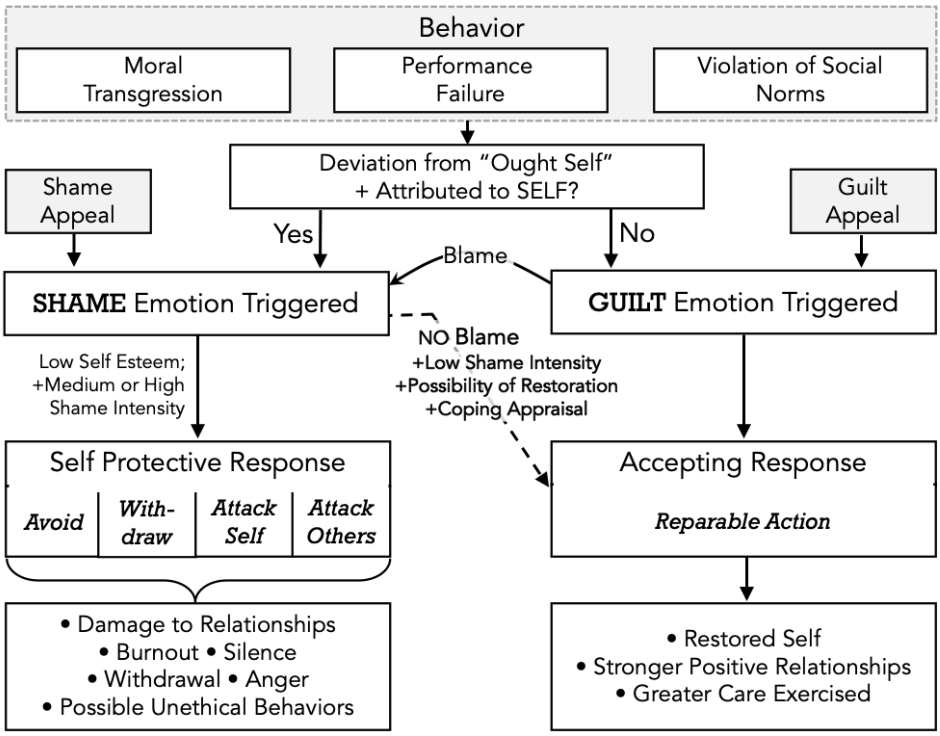

Figure 1: A Process Model of Shame (dashed line reflects rarity of that particular cross-over)

151], especially when an individual falls victim to a cyber attack [25, 33, 103]. People feel shame when they fall for a cyber scam [2, 6, 31]. Frik *et al.* [47] suggest encouraging goal setting to improve compliance, but admits that non-completion of a goal can produce feelings of disappointment and shame. Gafni and Pavel [48] also refer to the shame small businesses feel for experiencing a cyber attack, with Janjarasjit and Chan [67] reporting that customers would be more forgiving of a company that showed their sense of guilt and shame when they fall victim to a data breach.

Shame Prevents Cyber Crime Reporting: Anthony [6] points out that shame deters reporting. Kwak *et al.* [80] confirm that those who felt shame were less likely to report being Phished.

Advocating Blaming & Shaming: An Australian study [94] explored security policy options during a security exercise. They mention that some participants favored using a 'name and shame' tactic to respond to insecure behaviors. Falco [45] lists this tactic as one of his cybersecurity principles to improve the security baseline. Some believe that companies should be shamed for experiencing breaches [69, 89, 143].

The UK's National Cyber Security Centre (NCSC) [9] announced that government departments were going to be named and shamed for their cyber security failures. Stevens *et al.* [132] propose a dashboard of attacks, maintained by the NCSC, which might conceivably be used for this purpose [127]. A similar response is also favored by some authorities in the USA [32].

These are examples of a victim blaming strategy, which occurs in other contexts, including revenge porn [130] and rape [104]. Janoff-Bulman *et al.* [68] argues that the tendency to blame is a cognitive bias based on the blamer falling for the hindsight bias. Ruetenik [119] explains that the folly of victim blaming lies in the fact that it focuses on the individual rather than on the social situation that caused the adverse event. Moreover, pointing fingers at the individual also prevents the organization from identifying issues in the greater socio-technical system which will then remain to trip up other employees.

Consequences of Shaming: Zec's [158] interview study of SMEs, found that cyber security decisions could lead to feelings of guilt and shame, but more critically such responses then resulted in counterproductive behaviors at work. In a recent study Farshadkhah *et al.* [46] presented participants with scenarios that induced shame and guilt. They found that the presence of an onlooker could lead someone who was considering engaging in a non-compliant behavior to feel guilt and shame. Critically, only those who felt guilt reduced their intention to violate security policies.

Post-incident sanctions can produce strong negative emotional responses, including guilt, but more particularly shame when others learn why an employee is being prevented from doing their work for a period. These shaming experiences are likely to produce intense pain, derived from a public-raising self-consciousness, that can create negative psychological, physiological and societal consequences [34, 39, 55].

Baldwin *et al.* [11] found a relationship between an individuals' shame and a sense of reduced self-efficacy. This result is particularly of concern in the cyber security domain, where there is often a

generic deficit in cyber knowledge, and a feeling of reduced self-efficacy is likely to make the person feel even less able to carry out the desired actions.

Empirical Investigations: Studies into the impact of ''naming and shaming" responses reported that 70% of employees said that they would comply with policies if their non-compliance would be treated in this way [61] . On the other hand, Brennan and Binney [21] found that using negative emotions such as fear, guilt and shame, although it could exert a short-lived motivational influence, it was not self-sustaining; Rather, long-term responses were more typically self-protective or paralyzing. In response to these findings, they advise against the use of such emotions as a means of encouraging compliance. Similarly, Caldwell [26] warns against this approach in cyber security.

A study which *has* tested the impact of guilt and shame on future compliance failed to find any significant influence of shame on compliance intentions, but did show an influence from guilt [46]. However, their study used scenarios to assess an anticipated response. In contrast, this study sought to explore actual incidents in which people inadvertently triggered cyber security incidents, and had to cope with their very real aftermaths.

4 SURVEY

In this study, we investigate the impact of cyber security related shame in an organizational setting. Adam Smith [43] argued that people in poverty were ashamed of their poverty. This leads us to wonder whether people also experienced undeserved shame for having insufficient cyber-related expertise, or making honest mistakes that contributed to a cyber-related incident [120]. Our research questions were:

RQ1: *If someone non-maliciously triggers an adverse cyber security event, do they feel shame?*

RQ2: *If they felt shame, how did the way their line manager/employer handled the situation influence: (i) their relationship with their employer, and (ii) their long-term behaviors at work?*

The following section outlines the design of this study, including the survey developed to answer these research questions.

4.1 Survey Design

We developed the questionnaire (see Appendix A), inviting respondents to tell us whether they had been involved in triggering a cyber security event. Given that shame might cause people to hide their own behaviors, we also asked them if someone they knew had caused such an event, and asked them about what that person had told them about their experiences.

4.2 Participants

The survey was published on Amazon's Mechanical Turk (MTurk) and the Qualtrics survey platform was used to collect responses. Participants resided in the United States and were all 18 years of age, or older. They were compensated with $1, and offered bonuses for especially thoughtful responses to these open-ended questions. MTurk workers were advised on both the MTurk platform and throughout the survey of the potential for bonuses for providing especially thoughtful responses. The bonuses varied from $0.50 to $5.00. MTurk workers generally provide high-quality responses to survey data when certain quality control measures are put in place [131]. In particular, in this study multiple quality control questions were used, including a manual review of textual responses and cross-validation with other studies conducted that used higher worker qualifications. The initial worker qualifications we used in this study were quite low (50 HITS (human intelligence tasks) completed with a 95% approval rate or higher). This was done to maximise the participant pool eligible to participate in this survey given the specific types of experiences we were interested in. However, once the quality control issues became apparent with the data collected, we employed a much higher qualification level of 1,000 prior HITS with a 98% approval rating or higher as an additional quality control measure. This technique was possible through cross-validating with other studies that employed this higher worker requirement. If the Turker had successfully completed a prior study by one of the authors with this higher qualification level then they passed this cross-validation.

1,145 Turkers began our survey, with 1,072 successfully completing it. 73 participants were discarded for failing to complete satisfactorily one or more of these quality control questions. While 429 of these retained participants indicated that they had personally experienced a cybersecurity incident at work, only 53 were usable responses to these open-ended questions. These low numbers of retained open responses arose as some participants did not answer all of the questions, while other Turkers appeared to have employed automated systems to complete the process. The latter resulted in awkwardly worded, and difficult to decipher responses, that included several duplicates, and appeared to have been due to the use of automated web scraping that sought to identify possible answers to the open-ended questions.

Challenges associated with using MTurk is not new, but have become more prevalent in recent years [29, 74]. The problem is a result of automation, tools to expedite the process for Turkers, and a greater number of non-native English speakers from outside the United States using virtual private networks (VPNs) and other techniques to be able to participate in specific assignments [29, 72, 74, 150]. In addition to the recommendations noted by other researchers, we were able to increase our initial worker qualifications *ex post facto*.

A further 342 participants indicated they knew someone that had experienced such an incident. Through the same verification process, a final 107 usable responses remained to support analysis.

Demographics: Between these two questions (direct and indirect experiences), 124 participants provided usable responses. Most of these participants identified as male (63%) with 37% identifying as female. They were generally well-educated (71% held a Bachelor degree or higher) and younger (56% were between 18 and 39 years old) than the population at large. Most participants were White (68%), followed by Asian/Pacific Islander (18%), Black/African American (6%), Hispanic (4%), Other/Multi-Racial (2.4%), and Native American/Alaskan Native/Indigenous (1.6%). Overall, the demographics of our participants were similar to those found in other MTurk studies [42].

While we do not suggest that the participants that completed the survey are representative of the general population, they do nonetheless provide a good demographic cross-section of insight as it relates to possible feelings, experiences, issues, and behaviour related to the shame and guilt of employees in an organisational setting. Given the qualitative and exploratory nature of our data collection efforts and quality control issues inherent to a crowd-sourced platform as identified previously, we are hesitant to generalise to the MTurk population as a whole, let alone the broader population. Although MTurk workers do provide a more diverse participant pool compared to the traditional college course consisting of mostly sophomores [126], they do represent a unique population of individuals that choose to engage in this type of work activity to earn or supplement their income.

4.3 Analysis

Practically, we broadly followed Braun and Clarke's [20] four stages of thematic analysis: data familiarisation; initial code generation; thematic search and review; and defining and naming themes. Our retained responses were coded using open coding [133] assigning tentative codes to sections of data that captured reflections and discourse on pertinent issues relevant to our research questions. Through constant comparison and reflection on the possible links, we moved from inductive 'first-order codes' to 'second-order themes' [20] until no new substantive observations or linkages occurred. For example, identifying the emotions of respondents to discern those with negative emotional responses involving "shame" , "anger" , "anxiety" or "guilt" from those who felt more positive emotions including "confidence" and "excitement." We distinguished those who indicate self-sanctions "i didn't apply the training" from those who indicated a social sanction that arose from their colleagues such as "being judged by others for the behavior." The resultant coding was independently checked, verified or negotiated by two of the authors regarding the interpretation and their assignment to categories and wider themes. This recursive activity was undertaken following each participants' coding, and then again collectively on coding competition. Specifically, we drilled into areas of convergence and divergence to examine interpretations, analytical patterns and differences across these responses, thereby increasing analytical credibility. The themes that emerged are shown in Figure 2.

5 FINDINGS

Analysis of our qualitative survey responses revealed that events and their handling by the organization often resulted in feelings of shame (RQ1). Furthermore, we found there were consequences from these experiences for their employer relationship (RQ2:i), as well as subsequent behaviors at work (RQ2:ii), depending on what happened in the aftermath of the incident. These will now be discussed separately, drawing on our template analysis (see Figure 2) and illustrating themes using pertinent anonymous quotes.

5.1 Behavior

Fifty three participants mentioned experiencing a Phishing attack. Some said reported on a personal experience with others reporting Phishing-related incidents that involved an acquaintance or friend. This distinction is not necessarily reliable since people may report a personal experience as having happened to someone else, due to a sense of shame being triggered by the memory. This incidence is unsurprising given that Phishing attacks are so prevalent[2].

Four different types of emotions were reported as elicited from these experiences. Critically, the valence of all emotions were predominately negative, specifically: anxiety (17 respondents), shame (16 respondents) and anger (4 respondents). Thus we offer insight into our two research questions.

Reflection on these events indicates that they were associated with high levels of anxiety as the following quotes illustrates: "*I felt worried and upset that I was targeted*" (P1). Furthermore, phishing incidents also could induce anger, here directed at their vulnerabilities, but in other quotes towards perpetrators: "*I feel tensed and become angry about my device. I am out of control. My mood was totally bad at that situation.*" (P36)

Shame was a significant response captured by the next quote, induced initially from their own actions, in this case performance failures (lack of usual attention to detail and incompetence), and moral transgression (should have known). "*I accidentally opened an attachment that was on an email from someone I know, but I should have known they wouldn't have sent it. I felt stupid because I knew right away that I shouldn't have done it. I berated myself over it - I know that being meticulous is very good in my position, and I let haste interfere with that. It was no one's fault but my own. Luckily, our awesome IT guys were able to isolate it and keep any damage from happening. I swore, at that time, that I would ask them no matter how stupid I felt for the question.*" (P12)

There was a further component to this reaction that emerged from self-reflection, and is associated with a further rumination process, in which blame is attributed for the outcome (my fault). In this way, it is not just the organization's response that could elicit shame (**RQ1**). The earlier example (P12), however, reveals a remediating journey, which commenced with self-condemnation but could be transformed by the actions of key organizational actors (here IT) to result in a change to future behavior reducing the risk.

Recall of these various incidents indicates emotions were not isolated, instead co-occurring as the following quote illustrates, referencing feelings of shame and anxiety, and then guilt: "*I saw a pop up it is like a notification that my system has been infected with 49 viruses after clicking what looks like a Russian website link, then i was directed to click on "delete virus" or else my system will be shut down and i will lose my file in 60 seconds, I immediately did that and after doing that, 30 minutes later i couldn't log into my email and my Facebook account again, I felt like an idiot and i was scared. I was soo scared because it was my working laptop and full of company's data and work. I was also soo embarrassed, ashamed and guilty. I remember asking myself how i am going to tell my boss.*" (P54)

Thematic analysis scrutinizing these recollections reveals an important temporally-derived coding; first, these situations often included elements that show these individuals have been working at speed at the time they occurred, usually atypical haste (see earlier P12). Respondents reflected on how this caused a departure from their usual ways of working, reducing the time available to be detail-conscious, e.g. scrutinizing the sender's email address. These

[2]https://enterprise.verizon.com/en-gb/resources/reports/dbir/

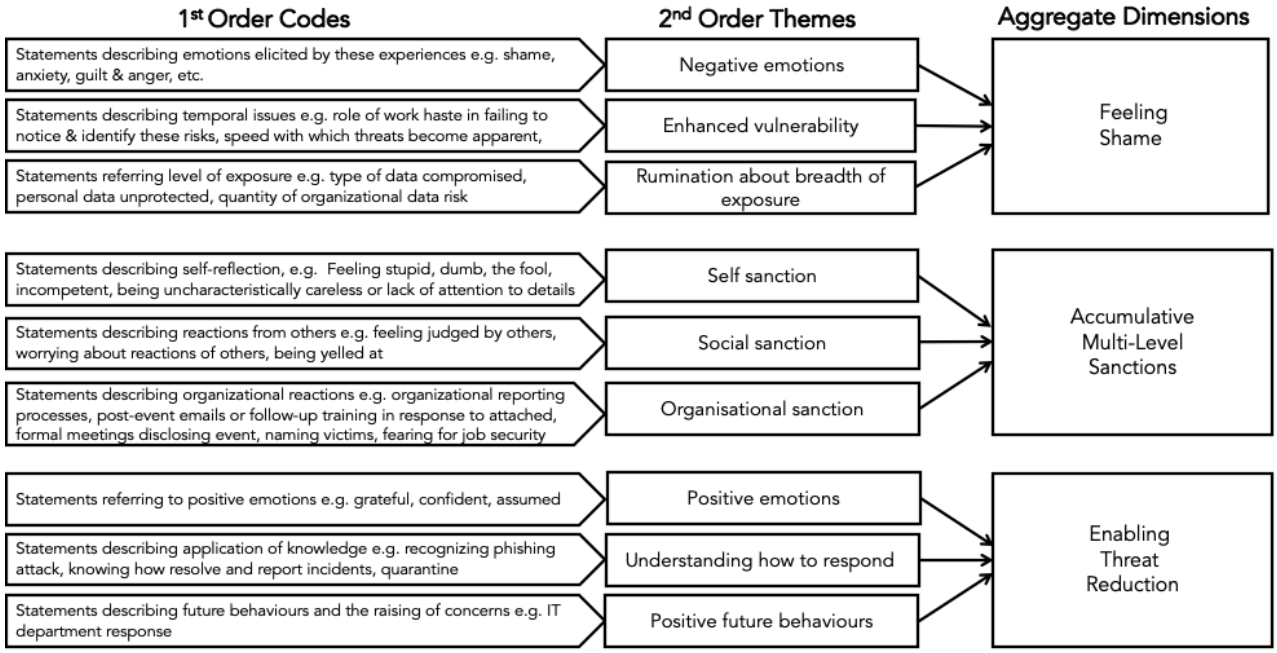

Figure 2: Thematic Analysis

insights suggest that organizational working practices might be a significant precursor, with participants' more rapid responses contributing to the elevation of threat levels. The next quote illustrates how these incidents were an aberration, and not typical of their usual working behaviors: "*I felt like a fool. I felt careless and questioning my attention to detail. I knew right away what I had done. I knew that normally I wouldn't have clicked what I had, but I was in a rush and recklessly clicked the option.*" (P22)

This temporal dimension is also apparent in the speed with which events unfolded (as denoted by P54). Together, these different temporal elements compound the individuals' sense of lack of control, with their computers dramatically freezing. In this moment they reveal a striking juxtaposition between their previous pace of work and its sudden curtailment. These pacing codes reflect an enhanced sense of vulnerability, which arose from the alienation of their normal working-self and working practices, and appears to heighten their risk of failing for such attacks.

A further theme associated with these shame emotions concerns their levels of exposure, specifically the types of data that are exposed, often including both personal, and company data and their work (see P54). Linked to the earlier temporal codes, the curtailment of their prior efficient and effective functioning in this dramatic fashion is accompanied by a stark rumination about the enormity of what has occurred and the potential harm to them and to their organizations. The following quote highlights the sense of very personal violation that befalls them: "*I felt compromised. violated digitally. Like I had lost my wallet. or someone had taken my house keys. And I did not know who this person was and what they would do.*" (P101)

A further consequence of their post-incident rumination is important and detrimental performance outcomes, compounded by reductions to their work motivation, and elevations in their anxiety derived from further speculative review of its wider impacts as the next quote denotes: "*I accidentally clicked on a link in an e-mail regarding having a voice mail message ... I felt dumb, and blamed myself at the time ... I felt less motivated to work that day ... I felt made me less productive that day. I also had increased anxiety and fears that something bad was going to happen organization-wide after I clicked on the link.*" (P31)

If left to proliferate, there are clear long-term consequences from these feelings of shame, adding further nuance to **RQ2(ii)** as the next quote captures: "*My co-worker took a month off to take care of his mental health because he felt so much shame and guilt regarding this situation.*" (P67)

5.2 Sanction

A striking feature of these incidents is the accumulation of multi-level sanctions. Analysis of the participants' accounts of these incidents identifies three distinct forms of sanctions, which, more critically, have a cumulative affect, further escalating their sense of mortification.

The first is *self-sanction*, where reflection of these incidents produces an attribution of blame as arising due to their own failures. This is evident earlier (see P12), with individuals berating themselves for causing these situations. The level of self-sanction often implies a moral transgression, that stems from an individual's failing despite receiving training as the following quotes reveal: "*I felt careless and very ashamed. My boss did not blame me but I felt incompetent.*" (P84) "*I felt really at risk and stupid for having clicked on the link provided in the e-mail message. I was angry at myself thinking that I should have known better. There was tons of training*

and advice given to us about fishing e-mails and still I clicked on a fraudulent link that opened us up to possible infection. I felt like I had let myself and my company down." (P72) "*I felt sort of embarrassed. I haven't been super vigilant about following my company's IT security policies and when I fell for a phishing scam that was sent to my company email address I felt like I should have paid better attention to the IT security training that we are mandated to take every year. I usually click through those trainings mindlessly but this experience of getting phished made me feel like I was responsible for this incident and should have been able to prevent it.*" (P58)

The severity of this self-sanction these shame-incidents produce can be intense, inducing a strong withdrawal response, as the next quote reveals:"*They felt really scared and depressed. They felt embarrassed and like they might lose their job. They clicked a link in a fishing email and put the companies data at risk. They wanted to climb into a hole. They actually didn't want to come back to work the next day. I had to talk them down from the ledge. ....They went to IT and told them what happened immediately. They apologized and promised to stay on top of things better. They felt ashamed, they wanted to hide under a rock. I felt really bad for them.*" (P47)

A second level of sanction stems directly, or indirectly, from concerns about the reactions of others to these incidents, to add a social sanction, as the next quotes illustrate; The first example reveals a clear blame attribution from others, and the second show how self-shame is amplified as attention switches to concern about their judgment both from generic 'others', and also critical key organizational actors, notably their line manager: "*they let in malware into their companies server and caused harm to their company.*" P104 "*I felt so bad and i couldn't believe i could ever fall for such, but i eventually did, which made me felt so sad and unhappy with myself, because i will be judge by others and my manger.*" (P40)

This cumulative inducement to feel ashamed arises from simply thinking about others' reactions as the next quote demonstrates, with the ignominy of a colleague's compromised work account exacerbated, both in level and its duration through a further mortification derived from the impoverished inducement they fell for: "*They mostly felt shame, because they fell for a phishing attack that simulated the login page to our work. This meant the person had full access to their account now. The offer was for free parking, which she felt even worse about since it wasn't even that enticing of an offer. They really felt bad for months after.*" (P16)

A third, and final, level of sanction can be added through the organization's responses. This theme confirms **RQ1** showing how the poor handling of these incidents can actively exacerbate feelings of shame. A central actor in these further responses is the manager, with numerous examples of poor reactions as the next quote illustrates: "*She was a nightmare manager and instead of handling it appropriately, she went on a witch hunt badgering all the other offices and raking my boss over the coals as a bad example of computer safety.*" (P85)

Shame could also be induced by virtue of the organization's communication processes, with employees aware that any renewed cyber security awareness-raising denoted that a successful phishing attack had occurred. Inadvertently, these communications could reveal the identities of employees as the next two quotes demonstrate: "*When someone falls for one of these attacks, there is often an email sent out from their address trying to do more phishing attacks. So everybody at the state knows when someone falls for it. We had one event in my agency (around 40 people) last year, and the poor lady who fell for it was horribly embarrassed by it.*" (P124) "*After they fixed it they sent out an email to all of us with a picture of the phishing scam and told us not to click the link. The picture had the email of the person who got the virus so we all know who fell for it... they were grateful that the problem was fixed, but they still felt a little hurt or embarrassed. They were basically called out in front of everyone because of this.*" (P10)

This proliferation of shame, as noted earlier (see P10) can be charted, with the next quote showing its rapid escalation and debilitating consequences to an individual's performance. These insights address two research questions showing clear consequences for employer relations (**RQ2(i)**) and to work behavior (**RQ2(ii)**). We can see shame-related production decline related to their own emotional responses, but then further exacerbated by their manager's incivility which overwhelms their cognitive resources and thereby blocks their subsequent capacity to respond to their co-workers' potential solutions. This short-term capability failure produces secondary wave of shame, which is exacerbated again by their line manager's subsequent distrust response of add a layer of monitoring to just *their* work: "*I felt so guilty at the moment. Because my superiors yelled me for this incident. I asked excuse many times. But they didn't accept my excuse. I tried to establish in front of others. In that moment, feel so sick and My thoughts are very scary and I have more confusion on the event. I tried to deviate from this event. In the moment, I feel so cold. Many of other members in my team suggested various ideas to solve this problem. But my mind didn't concentrate on anything. It only thought on employer's face reaction. How he reacts in this situation. After this incident, my employer warned me about this kind of events. Some times, he interrupt my work. and started to check my work. It was hurt me for few times. I had more trouble and get struggles by the single event. "* (P35)

The reduction in trust towards these employees is evident in a number of incidents, to reveal the emergence of a distrust spiral between the different parties, adding further nuance to **RQ2 (i and ii)** as captured in the following quote: "*She was not happy with the way it was handled. It was very stressful on her and she had to go in the office and explain what had happened. This made her feel distrust toward him because she felt that she was a trustworthy employee and after this she felt like they did not trust her any more.*" (P62)

While some formal organizational responses are not intended to be shame inducing, they can proliferate ripples of embarrassment for the individuals' implicated. The next quote reveals shame events' accumulative progressions, adding further insight for **RQ2**; specifically, we see reactions to a moral transgression (failure to get permission) producing an immediate social sanction (silence), that are further escalated by the line manager, who involves IT services (software fix), Human resources (formal warning and training), other staff (training), and more widely with the whole department loosing a day's production. Note too recognition of its increasing toll for this individual: "*It is necessary for us to gather some very personal data from our client. We have very rigorous electronic and paper filing systems that must be followed. One of my coworkers received an email about installing an antivirus app. We are NEVER to download anything without permission, but she did. We had a meeting later that week. During that meeting she casually mentioned something*

about how long it took to install the new antivirus app. Dead silence for a moment and then my supervisor dismissed everyone except that employee. She came to my desk later. It was clear she had been crying. Because of what she did, our office had to close early that day for our tech support team to purge our system and make sure no spyware had been installed. She had gotten a pretty severe talking to, got written up and caused the rest of us to have to attend additional training on office security. Our employer handled it pretty well. I did not envy her having to call her supervisor to tell her what happened. After speaking to my coworker, my supervisor called everyone back into the meeting room. While it had been pretty clear who was in trouble, without naming names, my supervisor said we would have the last 2 hours of the day off with pay while our tech support team worked on our system and to please clear our calendars for the first half of the next day for some required training. Giving my coworker credit, she owned her breech of the rules. She was beet red the rest of the day, but went about her business. She honestly thought she was going to be fired and was very grateful that she didn't. " (P26)

Without effective organizational interventions, these incidents can become triggers to others' responses - critically their decisions to quit. These reactions arise from either other organization's attempts to divest themselves of responsibility as illustrated in the first quote below, or from a resultant panic that leaves key actors unable to move on, as the second quote shows. In these cases, we gain insight into a further creep of shame, spreading to other employees who feel ashamed of the organization's poor treatment of their fellow workers: "*He felt that the employer at the time had not put in place adequate measures to combat the security breech risk and felt that they were blamed for a mistake that they did not really commit. He was not among those that were fired but he told me he resigned almost immediately due to the treatment they received.*" (P27) "*Instead of just sending out refresher training or calling a general group meeting, went office to office singly discussing the "infraction" in an over the top kind of panic holding my boss up as a negative perpetrator of what not to do. It was awful.Well, that particular boss eventually led to that person retiring from the company early. She went to work a harder job just to escape. And honestly, it didn't take me long to follow that example.*" (P85)

An outcome separately, but also accumulatively from these three forms of sanctions, is to stifle the individual's voice to admit what they have done. Whether from self-sanction, through fear of social ostracisation, or the line manager's verbal reprimands, these identify shortcomings that can have significant consequences for the individual. These distinct levels of shame reflect the ease with which it can proliferate within the organization, making its containment a challenge, to produce long-term detrimental consequences that extend far beyond the origin. These can affect a wide variety of others either directly by diverting their attention (e.g. those in IT services), or indirectly, in lost production or having to undertake remedial training. A contagion can form for shame derived from poor organizational responses, that lead other employees to feel shame at the shoddy treatment of their colleagues.

5.3 Constructive responses

In contrast to these negative outcomes, we also found examples of very positive outcomes. While in the minority, these responses are important and associated with divergent themes, compared to shame incidents. First, they have positive emotional tones. Second, they have distinct performance consequences, and finally, they reveal a productive reduction in risk behaviors, including increasing information sharing with key organizational actors. These three elements are captured in the next quote. " *I felt very confident on how to deal with the e-mail i received. I literally just deleted it and provided it to my IT dept at my work place.*" (P3)

Together these three themes denoted employees who felt able to reduce organizational phishing threats. Supervisors play a critical role in these positive responses, helping to calm the induced emotions, and, as the next quote illustrates, increasing organizational commitment and engagement: "*Most of the response was supervisors trying to calm her down and let her know that it happens and it's not something to get too worked up over. Honestly, the kind professionalism of our supervisors all the way up to my executive director is a big part of why my agency is so nice to work for..I definitely think she appreciates working for our agency even more as well, in some agencies that would have been dealt with harshly.*" (P124)

These positive cases reveal some distinct elements of contexts support, as the next two quotes capture. They show, in addition to a productive engagement with affected employees, a multi-strand approach that is designed to help the employee and the organization to learn from these incidents. They include: review of current employee competence, identification of specific training needs; development of simple incident protocols to avoid freeze responses, instead facilitating a remedial reaction; application of special software that confines these attacks; and the diminishing of unproductive diverting efforts to apportion blame, instead regarding such incidents as mistakes rather than more pervasive moral transgressions. "*After the employee shared what had happened, they worked with our IT department to make sure that that email address was blocked. They also reviewed with the employees how to recognize phishing emails and the protocol to follow if we receive one. I don't believe the employee was reprimanded. They still felt embarrassed but felt supported by our employer and motivated to do better in the future.*" (P84) "*We did have a piece of software get installed on our pcs however because of restricted permissions on the pc the software was not able to propagate to other devices. It was recognized and removed fairly quickly by the IT staff.*" (P13)

Through these elements, although shame is still present, it is more likely to be confined to initial self-sanction, through the responses of line managers. This then motivates more productive future employee behaviors, rather than propagating unproductive rumination. As a workplace, it is also likely to lead to greater resilience with employees seeing the benefits of raising concerns that they have made a mistake, rather than being afraid to report these concerns, thus remediation can commence more rapidly. Furthermore, these organizations are better able to contain any aforementioned shame contagion, and retain employees who have had an invaluable and memorable learning experience. These elements are captured by these final quotes: "*He felt that his fear, worries, and angry have been addressed adequately by the employer. Thus he felt that his confidence in the company has been renewed, as he felt that the company is more than able to protect everyone.*" (P22) "*He felt so much love for the employer for not making him look foolish and for defending him.*" (P84)

Interestingly closer scrutiny of accounts shows how some individuals have an unrealistic sense of their competence, which then rapidly dissolves into shame when they fall for the phishing attack, as the next quote illustrates. The example suggests the value of highlighting their vulnerabilities, and making employees aware that mastery takes time, and the right context (i.e. not rushing) to develop: "*I felt very silly because I expected that I would know how to spot a phishing email. I was embarrassed that I 'fell for it,' and worried/disappointed that I had created extra work for the IT team because of my inattention to detail.*" (P46)

6 DISCUSSION & REFLECTION

The first step in moving towards a more effective management of adverse events is to acknowledge that most employees intend to "do a good job" rather than to commit errors [38, p.99]. Moreover, that the cyber security context is complex and challenging, which makes it difficult for people to operate in an error-free fashion. As such, the employee should not be seen as the enemy; they are pitting their wits against a multitude of highly-skilled adversaries. They do not need further condemnation adding to their own self-sanctions; instead, they need support.

How the employer responds to such mistakes is crucial to the valence of the consequences, with further blaming and shaming creating long-term negative impacts. Positive non-blaming responses are found to have the potential to strengthen the organization as a whole.

The recommendations are grounded in the UK's National Cyber Security Centre's [99] "You shape security" guidance, and augmented using insights gained from responses to our survey. We ground our recommendations on this set of guidelines because they, in turn, have been built on the literature on Just Culture by Dekker [38], the research of Ashenden and Lawrence on Security Dialogues [8] and research into Shadow Security by Kirlappos, Parkin and Sasse [77], all of which have a similar approach to ours in treating employees justly.

(1) Implement a system for 'no-blame' security incident and near miss reporting: This recognizes three important realities. The **first** is that these kinds of mistakes can be made by anyone. P10, in reflecting on a colleague's shame inducing experiences, demonstrates this: "*They had felt really guilty and embarrassed. I understand why they clicked the link. The email handle looked really similar to those other employees have at our organization. The IT department had to send out an email to the entire staff telling them not to click links from outside the organization.*

The **second** is that near misses can help us to reveal vulnerabilities that can be addressed, thereby preventing a real incident later.

The **third** reality is that blame is corrosive and exacerbates how bad people feel anyway about what has happened, with no benefit attached to this. P43 highlights the intensity of these experiences and what powerful learning experiences they are in their own right, without necessitating the use of further shame. We see the clear behavioral change through showing care: "*"I genuinely felt physically nauseated and terrified that something horrible would come out of it. I rarely feel panicked but my body went into a form of total shock when I found that information had been compromised. However, it was resolved very quickly and the damage was fortunately minimal. Since that time, even with my personal data I have been far more cautious with how I protect it. It was a lesson well learned.... in general the responses were of concern and fear. Fortunately, most were kind and helpful although concerns were high and much was at stake.".* P67 talks about one of his/her colleagues: *"One of my co-workers had gotten some malware from their email. Apparently, my co-worker opened the malicious email from a stranger (not from a work-related email) and had gotten some malware. My co-worker felt a lot of guilt and shame for even falling for this but I don't blame them because most of the emails we receive are important and it's pertinent that we respond to most emails."*

If people are made to feel even worse after such an event long-term and health consequences could occur too: *"My co-worker took a month off to take care of his mental health because he felt so much shame and guilt regarding this situation."* Blaming only makes the blamer feel superior: it is a singularly unproductive response to human error [114].

(2) Listen to employees: the NCSC recommends capturing the inputs of employees and to engage in dialogue with employees In a shame context, where individuals can already feel paranoid, accurate and timely information can challenge and impede such responses. P33 says: *"I could tell that the higher ups were very concerned when they told us that we were not allowed to give any information to the press. We were kept largely in the dark so that we did not have any information to give, so we were mostly confused and a bit worried about what might happen to the tech department that we worked in. We were slightly concerned about the amount of work that will come in due to people calling and asking about the event."*

Employees need to be accurately informed so that speculation is diminished. Such speculation can damage employee-employer relationships, fuel shame contagion and increase widespread anxiety.

(3) Creative engagement is crucial: P16 outlines that care is not sufficient without specific training needs also being met "*The boss was actually really understanding, and immediately spoke about how it was getting hundreds of other people. There were no punishments, but a little education of phishing scams.*"

P58 reminds us that engagement with training is necessary: *"I felt like I should have paid better attention to the IT security trainings that we are mandated to take every year. I usually click through those trainings mindlessly but this experience of getting phished made me feel like I was responsible for this incident and should have been able to prevent it."*

Training delivery can become a box-checking exercise, often online, often solo, without support from colleagues. This is an impoverished approach, and the consequences can be damaging. Contrast this to face-to-face training which has been specifically designed to engage people and encourages creativity. Moreover, such face to face activities facilitate discussions with colleagues [112], and an opportunity to work as a team in this context.

(4) Humanize planned responses to incidents: The first step is for all managers to accept that mistakes happen, and that such mistakes are most often not deliberate, nor can they be prevented by following rules [160]. Having changed the organizational mindset, responses to incidents should be informed by this realization. Managers should make it clear that the incident could easily have

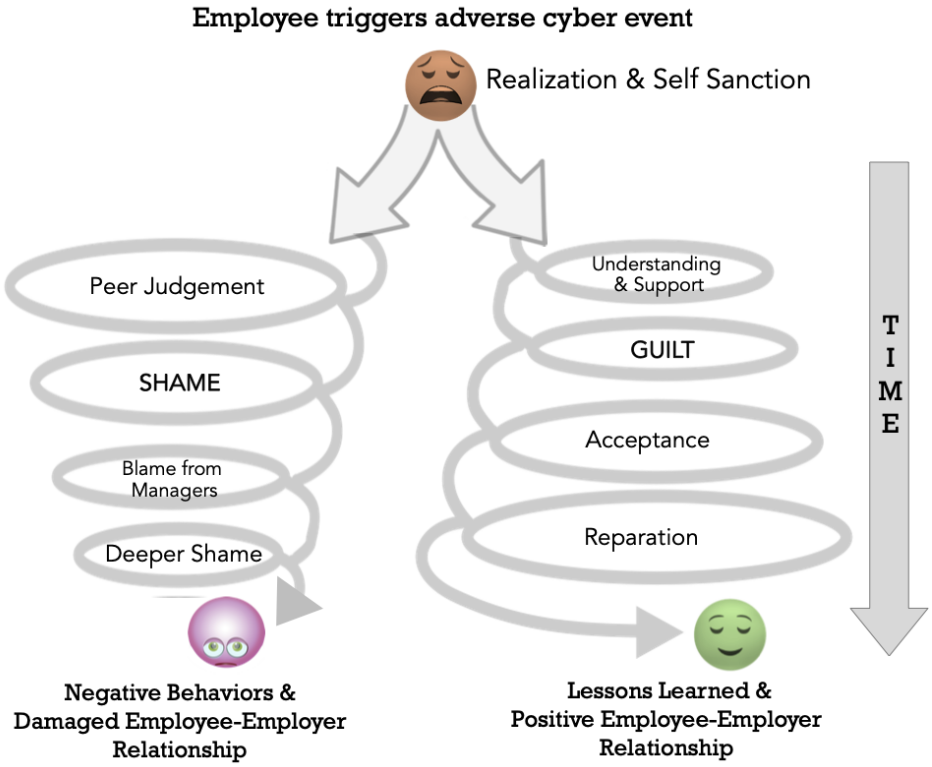

Figure 3: Outcomes depending on handling of event. The arrow on the left demonstrates the employee's downward spiral into despair, self-loathing and deeper shame. The one on the right demonstrates the employee's positivity resulting from their employer/manager's understanding and positive handling of the incident. (Spirals by Loren Kellen from https://commons.wikimedia.org/wiki/File:Espiral_Ascendente_Furac%C3%A3o.png)

happened to anyone else in the organization, so that the employee does not blame themselves and internalize a sense of shame with its roots in "*I* am the stupid one." The organization could consider facilitating a peer support network populated by employees who have been similarly duped by scammers in the past.

Training in de-escalation of shame should be included in line managers' and IT first responders' training and development. These are one of the most significant means to starting the positive spiral (see Figure 3 (right)); Their reactions can prevent others from seeing blaming and shaming of the individual as a legitimate and productive response.

(5) Experimenting by eliciting shame is likely to be unethical: Our investigation shows the severe and long-term consequences of felt shame. Given that shame is derived from people feeling that their standing in their in-group has been compromised, anyone hoping to study the effects of shame would have to trigger shame. Given what we know about the long-term deleterious impact of shame, it is unlikely that any convincing justification could be advanced for ethically experimenting with shame in the cyber security context.

6.1 Limitations

All the responses we analysed are based on recall, after the fact. While it would have been better to collect information during the shaming event, this option might well be infeasible. Indeed, prior study shows the nature of these events makes the memory open to recall as the resultant rumination makes it more resistant to decay [82]. Furthermore, organizations are unlikely to tolerate the presence and questions of researchers while they are trying to recover from an adverse cyber incident. A qualitative-only analysis is warranted for this exploratory investigation where we are seeking to reveal themes, not to confirm or deny hypotheses. Future work is planned that tests these using quantitative study.

7 CONCLUSION

Increasingly, organizations experience cyber attacks, with many caused by employee errors. These are painful experiences for everyone, and it is understandable that immediate responses can attempt to identify, and possibly blame and shame, those deemed responsible. Our investigation into the nature of shame, and its application in the cyber security domain, clearly shows that such a response can hurt the employee, and create further and wider unintended responses such as the processes and contagion induced by shame. It

can be detrimental to mental health, extending into personal lives, and destroying relationships with employers.

We also reveal how a positive response to a breach, even one that was caused by the employee, engenders more constructive outcomes, strengthening the employee-employer relationship, and promoting greater organizational commitment. Our findings make it clear that organizations' responses that incorporate shaming are counter-productive. They should be abandoned by any employer interested in the well-being of their employees, and the future resilience of their own organization to cyber attacks.

We conclude by returning to the question posed in the title. We have empirically shown shame to be an unpredictable and counterproductive foil. Those who blame and shame in response to honest employee mistakes in the cyber realm harm their employees *and* themselves in both the short- and long-term.

REFERENCES

[1] J. A. Abe. Shame, guilt, and personality judgment. *Journal of Research in Personality*, 38(2):85–104, 2004.

[2] I. Agrafiotis, J. R. Nurse, M. Goldsmith, S. Creese, and D. Upton. A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate. *Journal of Cybersecurity*, 4(1):tyy006, 2018.

[3] N. Agrawal and A. Duhachek. Emotional compatibility and the effectiveness of antidrinking messages: A defensive processing perspective on shame and guilt. *Journal of Marketing Research*, 47(2):263–273, 2010.

[4] E. Ahmed, N. Harris, J. Braithwaite, and V. Braithwaite. *Shame management through reintegration*. Cambridge University Press, Cambridge, UK, 2001.

[5] M. Alvesson and H. Willmott. Identity regulation as organizational control: Producing the appropriate individual. *Journal of Management Studies*, 39(5):619–644, 2002.

[6] Anthony. Why blaming and shaming are bad for cyber security, 2019. Retrieved 4 April 2021 from: https://blog.tmb.co.uk/blaming-and-shaming-threats-to-cyber-security.

[7] Aristotle. *Art of Rhetoric*. Simon and Schuster, Cambridge, MA, 1926. Loeb Classical Library 193. Translated by J. H. Freese.

[8] D. Ashenden and D. Lawrence. Security dialogues: Building better relationships between security and business. *IEEE Security & Privacy*, 14(3):82–87, 2016.

[9] W. Ashford. Government to name and shame departments failing to secure email, 2016. Retrieved 17 July 2021 from: https://www.computerweekly.com/news/450400935/Government-to-name-and-shame-departments-failing-to-secure-email.

[10] R. P. Bagozzi, W. Verbeke, and J. C. Gavino Jr. Culture moderates the self-regulation of shame and its effects on performance: the case of salespersons in The Netherlands and the Philippines. *Journal of Applied Psychology*, 88(2):219–233, 2003.

[11] K. M. Baldwin, J. R. Baldwin, and T. Ewald. The relationship among shame, guilt, and self-efficacy. *American Journal of Psychotherapy*, 60(1):1–21, 2006.

[12] A. Bandura. Social cognitive theory: An agentic perspective. *Annual Review of Psychology*, 52(1):1–26, 2001.

[13] R. F. Baumeister and D. M. Tice. Self-esteem and responses to success and failure: Subsequent performance and intrinsic motivation. *Journal of Personality*, 53(3):450–467, 1985.

[14] BBC. Company sues worker who fell for email scam, 2019. Retrieved 2 January 2021 from: https://www.bbc.com/news/uk-scotland-glasgow-west-47135686.

[15] I. Becheur, H. Dib, D. Merunka, and P. Valette-Florence. Emotions of fear, guilt or shame in anti-alcohol messages: Measuring direct effects on persuasion and the moderating role of sensation seeking. In S. Borghini, M. A. McGrath, and C. Otnes, editors, *E-European Advances in Consumer Research Volume 8*, pages 99–106. Association for Consumer Research, Duluth, MN, 2007.

[16] H. Behrendt and R. Ben-Ari. The positive side of negative emotion: The role of guilt and shame in coping with interpersonal conflict. *Journal of Conflict Resolution*, 56(6):1116–1138, 2012.

[17] M. Boiger, S. De Deyne, and B. Mesquita. Emotions in "the world": cultural practices, products, and meanings of anger and shame in two individualist cultures. *Frontiers in Psychology*, 4:867, 2013.

[18] J. M. Bonner, R. L. Greenbaum, and M. J. Quade. Employee unethical behavior to shame as an indicator of self-image threat and exemplification as a form of self-image protection: The exacerbating role of supervisor bottom-line mentality. *Journal of Applied Psychology*, 102(8):1203, 2017.

[19] V. Boudewyns, M. M. Turner, and R. S. Paquin. Shame-free guilt appeals: Testing the emotional and cognitive effects of shame and guilt appeals. *Psychology & Marketing*, 30(9):811–825, 2013.

[20] V. Braun and V. Clarke. Using thematic analysis in psychology. *Qualitative Research in Psychology*, 3(2):77–101, 2006.

[21] L. Brennan and W. Binney. Fear, guilt, and shame appeals in social marketing. *Journal of Business Research*, 63(2):140–146, 2010.

[22] S. M. Breugelmans and Y. H. Poortinga. Emotion without a word: Shame and guilt among Rarámuri Indians and rural Javanese. *Journal of Personality and Social Psychology*, 91(6):1111–1122, 2006.

[23] D. R. Brookes. Shame vs. guilt: Is there a difference? In *Beyond Harm: Towards Justice, Peace and Healing*, pages 143–51. Relational Approaches, 2019.

[24] M. Button and C. Cross. *Cyber frauds, scams and their victims*. Taylor & Francis, London, UK, 2017.

[25] M. Button, L. Sugiura, D. W. J. Shepherd, D. Blackbourn, V. Wang, and R. Kapend. Victims of computer misuse: Executive summary, 2020. Retrieved 3 April 2021 from: https://researchportal.port.ac.uk/portal/files/20818541/Victims_of_Computer_Misuse_Executive_Summary.pdf.

[26] T. Caldwell. Making security awareness training work. *Computer Fraud & Security*, 2016(6):8–14, 2016.

[27] A. B. Carlsson. Shame and attributability. *Oxford Studies in Agency and Responsibility*, 6:112–39, 2019.

[28] A. E. Carroll. Yes, people are traveling for the holidays. stop shaming them, 2020. Retrieved 5 April 2021 from: https://www.nytimes.com/2020/12/04/opinion/covid-holiday-travel.html.

[29] M. Chmielewski and S. C. Kucker. An MTurk crisis? Shifts in data quality and the impact on study results. *Social Psychological and Personality Science*, 11(4):464–473, 2020.

[30] M. Chrdileli and T. Kasser. Guilt, shame, and apologizing behavior: A laboratory study. *Personality and Individual Differences*, 135:304–306, 2018.

[31] A. Coluccia, A. Pozza, F. Ferretti, F. Carabellese, A. Masti, and G. Gualtieri. Online romance scams: Relational dynamics and psychological characteristics of the victims and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health: CP & EMH*, 16:24–35, 2020.

[32] P. Cowan. WA auditor could name and shame worst infosec offenders, 2016. Retrieved 17 July 2021 from: https://www.itnews.com.au/news/wa-auditor-could-name-and-shame-worst-infosec-offenders-421143.

[33] C. Cross. No laughing matter: Blaming the victim of online fraud. *International Review of Victimology*, 21(2):187–204, 2015.

[34] M. A. Daniels and S. L. Robinson. The shame of it all: A review of shame in organizational life. *Journal of Management*, 45(6):2448–2473, 2019.

[35] I. E. De Hooge, S. M. Breugelmans, F. M. Wagemans, and M. Zeelenberg. The social side of shame: Approach versus withdrawal. *Cognition and Emotion*, 32(8):1671–1677, 2018.

[36] I. E. De Hooge, M. Zeelenberg, and S. M. Breugelmans. Restore and protect motivations following shame. *Cognition and Emotion*, 24(1):111–127, 2010.

[37] R. L. Dearing, J. Stuewig, and J. P. Tangney. On the importance of distinguishing shame from guilt: Relations to problematic alcohol and drug use. *Addictive Behaviors*, 30(7):1392–1404, 2005.

[38] S. Dekker. *Just Culture: Balancing Safety and Accountability*. Ashgate Publishing, Ltd., Florida, USA, 2012.

[39] S. S. Dickerson, T. L. Gruenewald, and M. E. Kemeny. When the social self is threatened: Shame, physiology, and health. *Journal of Personality*, 72(6):1191–1216, 2004.

[40] W. Douglas Creed, B. A. Hudson, G. A. Okhuysen, and K. Smith-Crowe. Swimming in a sea of shame: Incorporating emotion into explanations of institutional reproduction and change. *Academy of Management Review*, 39(3):275–301, 2014.

[41] A. Duhachek, N. Agrawal, and D. Han. Guilt versus shame: Coping, fluency, and framing in the effectiveness of responsible drinking messages. *Journal of Marketing Research*, 49(6):928–941, 2012.

[42] M. Dupuis, B. Endicott-Popovsky, and R. Crossler. An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud. In *International Conference on Cloud Security Management*, pages 10–17, Oct 2013.

[43] Economist's View. Adam Smith on Poverty. Retrieved 17 July 2021 from: https://economistsview.typepad.com/economistsview/2008/06/adam-smith-on-p.html.

[44] J. Elison. Shame and guilt: A hundred years of apples and oranges. *New Ideas in Psychology*, 23(1):5–32, 2005.

[45] G. Falco. The vacuum of space cyber security. In *AIAA SPACE and Astronautics Forum and Exposition*, page 5275, 17-19 September, Orlando, FL, 2018.

[46] S. Farshadkhah, C. Van Slyke, and B. Fuller. Onlooker effect and affective responses in information security violation mitigation. *Computers & Security*, 100:102082, 2021.

[47] A. Frik, S. Egelman, M. Harbach, N. Malkin, and E. Peer. Better late (r) than never: increasing cyber-security compliance by reducing present bias. In *Symposium on Usable Privacy and Security*, pages 12–14, 2018.

[48] R. Gafni and T. Pavel. The invisible hole of information on SMB's cybersecurity. *Online Journal of Applied Knowledge Management (OJAKM)*, 7(1):14–26, 2019.

[49] S. P. Garvey. Can shaming punishments educate? *The University of Chicago Law Review*, 65(3):733–794, 1998.

[50] M. Ghorbani, Y. Liao, S. Çayköylü, and M. Chand. Guilt, shame, and reparative behavior: The effect of psychological proximity. *Journal of Business Ethics*, 114(2):311–323, 2013.

[51] M. Gibson. The role of pride, shame, guilt, and humiliation in social service organizations: A conceptual framework from a qualitative case study. *Journal of Social Service Research*, 45(1):112–128, 2019.

[52] P. Gilbert. Evolution, social roles, and the differences in shame and guilt. *Social Research: An International Quarterly*, 70(4):1205–1230, 2003.

[53] G. Graff. The name of the game is shame: The effects of slavery and its aftermath. *The Journal of Psychohistory*, 39(2):133–144, 2011.

[54] R. Greenbaum, J. Bonner, T. Gray, and M. Mawritz. Moral emotions: A review and research agenda for management scholarship. *Journal of Organizational Behavior*, 41(2):95–114, 2020.

[55] T. L. Gruenewald, M. E. Kemeny, N. Aziz, and J. L. Fahey. Acute threat to the social self: Shame, social self-esteem, and cortisol activity. *Psychosomatic Medicine*, 66(6):915–924, 2004.

[56] P. Hacker. Shame, embarrassment, and guilt. *Midwest Studies in Philosophy*, 41:202–224, 2017.

[57] J. Haidt. *The Righteous Mind*. Penguin, Great Britain, 2012.

[58] D. Han, A. Duhachek, and N. Agrawal. Emotions shape decisions through construal level: The case of guilt and shame. *Journal of Consumer Research*, 41(4):1047–1064, 2014.

[59] D. W. Harder. Shame and guilt assessment, and relationships of shame-and guilt-proneness to psychopathology. In J. P. Tangney and K. W. Fischer, editors, *Self-conscious emotions: The psychology of shame, guilt, embarrassment, and pride*, page 368–392. Guilford Press, 1995.

[60] S. Hareli, N. Shomrat, and N. Biger. The role of emotions in employees' explanations for failure in the workplace. *Journal of Managerial Psychology*, 20(8):663–680, 2005.

[61] M. Harris and S. Furnell. Routes to security compliance: Be good or be shamed? *Computer Fraud & Security*, 2012(12):12–20, 2012.

[62] P. Harvey, M. J. Martinko, and N. Borkowski. Justifying deviant behavior: The role of attributions and moral emotions. *Journal of Business Ethics*, 141(4):779–795, 2017.

[63] Helpnet Security. 4 in 10 organizations punish staff for cybersecurity errors, 2019. Retrieved 2 Jan 2021 from: https://www.helpnetsecurity.com/2020/08/05/4-in-10-organizations-punish-staff-for-cybersecurity-errors/.

[64] E. T. Higgins. Self-discrepancy: a theory relating self and affect. *Psychological Review*, 94(3):319–340, 1987.

[65] D. Y.-F. Ho, W. Fu, and S. M. Ng. Guilt, shame and embarrassment: Revelations of face and self. *Culture & Psychology*, 10(1):64–84, 2004.

[66] K. Jaffe, A. Flórez, M. Manzanares, R. Jaffe, C. M. Gomes, D. Rodríguez, and C. Achury. On the bioeconomics of shame and guilt. *Journal of Bioeconomics*, 17(2):137–149, 2015.

[67] S. Janjarasjit and S. H. Chan. Reaction of users as potential victims of information security breach. *Information & Computer Security*, 29(1):187–206, 2021. https://doi.org/10.1108/ICS-07-2020-0118.

[68] R. Janoff-Bulman, C. Timko, and L. L. Carli. Cognitive biases in blaming the victim. *Journal of Experimental Social Psychology*, 21(2):161–177, 1985.

[69] E. T. Jensen. President Obama and the changing cyber paradigm. *Admin. & Reg. L. News*, 37:3–4, 2011.

[70] C. G. Jung, S. E. Shamdasani, M. T. Kyburz, and J. T. Peck. *The red book: Liber novus*. WW Norton & Co, 2009.

[71] J. Kador. *Effective apology: Mending fences, building bridges, and restoring trust*. Barrett-Koehler Publishers, San Francisco, USA, 2010.

[72] T. Kaplan, S. Saito, K. Hara, and J. P. Bigham. Striving to earn more: a survey of work strategies and tool use among crowd workers. In *Sixth AAAI Conference on Human Computation and Crowdsourcing*, 2018.

[73] A. Kasabova. From shame to shaming: Towards an analysis of shame narratives. *Open Cultural Studies*, 1(1):99–112, 2017.

[74] R. Kennedy, S. Clifford, T. Burleigh, P. D. Waggoner, R. Jewell, and N. J. Winter. The shape of and solutions to the mturk quality crisis. *Political Science Research and Methods*, 8(4):614–629, 2020.

[75] M. F. Kets de Vries. *Down the Rabbit Hole of Leadership*. Palgrave Macmillan, Switzerland, 2017.

[76] A. Kirchner, M. Boiger, Y. Uchida, V. Norasakkunkit, P. Verduyn, and B. Mesquita. Humiliated fury is not universal: the co-occurrence of anger and shame in the United States and Japan. *Cognition and Emotion*, 32(6):1317–1328, 2018.

[77] I. Kirlappos, S. Parkin, and M. A. Sasse. "shadow security" as a tool for the learning organization. *Acm Sigcas Computers and Society*, 45(1):29–37, 2015.

[78] E. Kobayashi, H. Grasmick, and G. Friedrich. A cross-cultural study of shame, embarrassment, and management sanctions as deterrents to noncompliance with organizational rules. *Communication Research Reports*, 18(2):105–117, 2001.

[79] E. Kosofsky Sedgwick, A. Frank, and I. Alexander. Shame and its sisters: A Silvan Tomkins reader. *Duke Univerisity Press*, 1995.

[80] Y. Kwak, S. Lee, A. Damiano, and A. Vishwanath. Why do users not report spear phishing emails? *Telematics and Informatics*, 48:101343, 2020.

[81] C. W. Leach and A. Cidam. When is shame linked to constructive approach orientation? A meta-analysis. *Journal of Personality and Social Psychology*, 109(6):983–1002, 2015.

[82] M. R. Leary, C. Springer, L. Negel, E. Ansell, and K. Evans. The causes, phenomenology, and consequences of hurt feelings. *Journal of Personality and Social Psychology*, 74(5):1225–1237, 1998.

[83] K. P. Leith and R. F. Baumeister. Why do bad moods increase self-defeating behavior? Emotion, risk tasking, and self-regulation. *Journal of Personality and Social Psychology*, 71(6):1250–1267, 1996.

[84] H. B. Lewis. Shame and guilt in neurosis. *Psychoanalytic Review*, 58(3):419–438, 1971.

[85] M. Lewis. *Shame: The exposed self*. Harvard University Press, New York, USA, 1995.

[86] B. Lickel, K. Kushlev, V. Savalei, S. Matta, and T. Schmader. Shame and the motivation to change the self. *Emotion*, 14(6):1049–1061, 2014.

[87] J. Lindsay-Hartz, J. De Rivera, and M. F. Mascolo. Differentiating guilt and shame and their effects on motivation. In P. Tangney and K. Fischer, editors, *Self-conscious emotions: The psychology of shame, guilt, embarrassment, and pride*. Guilford Press, 1995.

[88] E. Livne-Ofer, J. A. Coyle-Shapiro, and J. L. Pearce. Eyes wide open: Perceived exploitation and its consequences. *Academy of Management Journal*, 62(6):1989–2018, 2019.

[89] J. Loeb. If you're not doing it… why the hell not? *Engineering & Technology*, 12(3):36–39, 2017.

[90] J. P. Martens, J. L. Tracy, and A. F. Shariff. Status signals: Adaptive benefits of displaying and observing the nonverbal expressions of pride and shame. *Cognition & Emotion*, 26(3):390–406, 2012.

[91] A. Maslow and R. Frager. *Motivation and Personality*. New York: Harper and Row, 1987.

[92] D. Merunka, I. Becheur, H. Dib, and P. Valette-Florence. Modeling and measuring the impact of fear, guilt and shame appeals on persuasion for health communication: a study of anti-alcohol messages directed at young adults, 2007. Euromed Marseille Working Paper. Retrieved 8 May 2021 from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=963593.

[93] J. Middelton-Moz. *Shame & Guilt: Masters of disguise*. Health Communications Inc, Deerfield Beach, Florida, 2020.

[94] I. Mikolic-Torreira, D. Snyder, M. Price, D. Shlapak, S. Beaghley, M. Bishop, S. Harting, J. Oberholtzer, S. Pettyjohn, C. Weinbaum, and E. Westerman. Exploring Cyber Security Policy Options in Australia. Technical report, Rand Corp Arlington VA Arlington USA, 2017.

[95] R. S. Miller and J. P. Tangney. Differentiating embarrassment and shame. *Journal of Social and Clinical Psychology*, 13(3):273–287, 1994.

[96] M. W. Morris and D. Keltner. How emotions work: The social functions of emotional expression in negotiations. *Research in Organizational Behavior*, 22:1–50, 2000.

[97] S. A. Murphy and S. Kiffin-Petersen. The exposed self: A multilevel model of shame and ethical behavior. *Journal of Business Ethics*, 141(4):657–675, 2017.

[98] D. L. Nathanson. *Shame and Pride: Affect, sex, and the birth of the self*. Norton, New York, 1992.

[99] National Cyber Security Centre (NCSC). You shape security, 2019. Retrieved 23 July 2021 from: https://www.ncsc.gov.uk/collection/you-shape-security.

[100] S. H. Nguyen. *Factors in the effectiveness of anticipatory guilt and shame appeals on health communications: The role of self-construal, regulatory focus and personal cultural orientation*. PhD thesis, Marketing, Victoria University of Wellington, 2017.

[101] P. M. Niedenthal, J. P. Tangney, and I. Gavanski. "If only I weren't" versus "If only I hadn't": Distinguishing shame and guilt in counterfactual thinking. *Journal of Personality and Social Psychology*, 67(4):585–595, 1994.

[102] U. Orth, R. W. Robins, and C. J. Soto. Tracking the trajectory of shame, guilt, and pride across the life span. *Journal of Personality and Social Psychology*, 99(6):1061–1071, 2010.

[103] Y.-F. Paat and C. Markham. Digital crime, trauma, and abuse: Internet safety and cyber risks for adolescents and emerging adults in the 21st century. *Social Work in Mental Health*, 19(1):18–40, 2021.

[104] C. M. Pinciotti and H. K. Orcutt. Understanding gender differences in rape victim blaming: The power of social influence and just world beliefs. *Journal of Interpersonal Violence*, 36(1-2):255–275, 2021.

[105] M. Pivetti, M. Camodeca, and M. Rapino. Shame, guilt, and anger: Their cognitive, physiological, and behavioral correlates. *Current Psychology*, 35(4):690–699, 2016.

[106] M. Plate. Shame and the undoing of leadership–an analysis of shame in organizations. In C. E. J. Hartel, W. J. Zerbe, and N. M. Ashkanasy, editors, *New ways of studying emotions in organizations*, volume 11, pages 81–107. Emerald Group Publishing Limited, Bingley, 2015.

[107] J. Pollard. Victim blaming won't stop global ransomware attacks, 2017. Retrieved 17 July 2021 from: https://go.forrester.com/blogs/17-06-27-victim_blaming_wont_stop_global_ransomware_attacks/?cm_mmc=RSS-_-BT-_-59-_-blog_10584.

[108] C. Poulson. Shame and work. In N. Ashkanazy, C. Hartel, , and W. Zerbe, editors, *Emotions in the workplace: research, theory , and practice*, chapter 19, pages 250–271. Quorum Books, Westport, CT, 2000.
[109] W. Presthus and K. F. Sønslien. An analysis of violations and sanctions following the GDPR. *International Journal of Information Systems and Project Management*, 9(1):38–53, 2021.
[110] J. Pridmore and T. A. Oomen. A Practice-Based Approach to Security Management: Materials, Meaning and Competence for Trainers of Healthcare Cybersecurity. In *International Security Management*, pages 357–369. Springer, 2020.
[111] J. Reason. Human error: models and management. *British Medical Journal*, 320(7237):768–770, 2000.
[112] K. Renaud. Cyber security is a team effort. *Network Security*, July:20, 2021.
[113] K. Renaud and M. Dupuis. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop*, pages 42–56, Costa Rica, 2019.
[114] K. Renaud, A. Musarurwa, and V. Zimmermann. Contemplating blame in cyber security. In *16th International Conference on Cyber Warfare and Security*, pages 309–317. Academic Conferences Limited, 2021.
[115] K. Renaud, V. Zimmermann, T. Schürmann, and C. Böhm. Exploring cybersecurity-related emotions and finding that they are challenging to measure. *Humanities and Social Sciences Communications*, 8(1):1–17, 2021.
[116] T. E. Robertson, D. Sznycer, A. W. Delton, J. Tooby, and L. Cosmides. The true trigger of shame: Social devaluation is sufficient, wrongdoing is unnecessary. *Evolution and Human Behavior*, 39(5):566–573, 2018.
[117] E. L. Rosenblatt. Fear and Loathing: Shame, Shaming, and Intellectual Property. *DePaul L. Rev.*, 63:1–48, 2013.
[118] T. Rothmund and A. Baumert. Shame on me: Implicit assessment of negative moral self-evaluation in shame-proneness. *Social Psychological and Personality Science*, 5(2):195–202, 2014.
[119] T. Ruetenik. Victim Blaming and Victim-Blaming Shaming. *Cultura*, 16(1):91–101, 2019.
[120] M. Rukgaber. Being in and excluded from the Sociotechnical World. In C. Mun, editor, *Interdisciplinary Perspectives on Shame*. Lexington, London, 2019.
[121] A. Saarelainen. Can guilt and shame-induced marketing encourage environmentally conscious consumption? a quantitative study on consumer response to negative emotional appeals in green advertising, 2018. Bachelors Thesis, Aalto University School of Business.
[122] R. Sadeghein. *Shame and Guilt: The Good, the Bad, and the Ugly*. PhD thesis, Marketing, West Virginia University, 2019.
[123] T. Scheff. The s-word is taboo: shame is invisible in modern societies. *Journal of General Practice*, 4(1):1–6, 2016.
[124] M. Schoenleber, H. Berenbaum, and R. Motl. Shame-related functions of and motivations for self-injurious behavior. *Personality Disorders: Theory, Research, and Treatment*, 5(2):204–211, 2014.
[125] W. R. Scott. *Institutions and Organizations. Ideas, Interests and Identities*. Sage, Los Angeles, USA, 2014.
[126] D. O. Sears. College sophomores in the laboratory: Influences of a narrow data base on social psychology's view of human nature. *Journal of Personality and Social Psychology*, 51(3):515, 1986.
[127] S. Shah. Government should name and shame companies with poor cyber security, say academics, 2019. Retrieved 17 July 2021 from: https://www.forbes.com/sites/soorajshah/2019/01/22/government-should-name-and-shame-companies-with-poor-cyber-security-say-academics/.
[128] D. W. Shin, J. H. Park, S. Y. Kim, E. W. Park, H. K. Yang, E. Ahn, S. M. Park, Y. J. Lee, M. C. Lim, and H. G. Seo. Guilt, censure, and concealment of active smoking status among cancer patients and family members after diagnosis: a nationwide study. *Psycho-Oncology*, 23(5):585–591, 2014.
[129] R. K. Sinha and N. Mandel. Preventing digital music piracy: the carrot or the stick? *Journal of Marketing*, 72(1):1–15, 2008.
[130] T. S. Starr and T. Lavis. Perceptions of revenge pornography and victim blame. *International Journal of Cyber Criminology*, 12(2):427–438, 2018.
[131] Z. R. Steelman, B. I. Hammer, and M. Limayem. Data collection in the digital age: Innovative alternatives to student samples. *MIS Quarterly*, 38(2):355–378, 2014.
[132] T. Stevens, K. O'Brien, R. Overill, B. Wilkinson, T. Pildegovičs, and S. Hill. Uk active cyber defence, 2019. Retrieved 4 April 2021 from: https://www.kcl.ac.uk/policy-institute/assets/uk-active-cyber-defence.pdf.
[133] A. Strauss and J. Corbin. *Basics of Qualitative Research Techniques*. Sage, Los Angeles, 1998.
[134] D. Sznycer, J. Tooby, L. Cosmides, R. Porat, S. Shalvi, and E. Halperin. Shame closely tracks the threat of devaluation by others, even across cultures. *Proceedings of the National Academy of Sciences*, 113(10):2625–2630, 2016.
[135] J. P. Tangney and R. L. Dearing. *Shame and guilt*. Guilford Press, New York, USA, 2003.
[136] J. P. Tangney, J. Stuewig, and D. J. Mashek. Moral emotions and moral behavior. *Annu. Rev. Psychol.*, 58:345–372, 2007.
[137] J. P. Tangney, P. E. Wagner, D. Hill-Barlow, D. E. Marschall, and R. Gramzow. Relation of shame and guilt to constructive versus destructive responses to anger across the lifespan. *Journal of Personality and Social Psychology*, 70(4):797–809, 1996.
[138] G. Taylor. *Pride, shame, and guilt: Emotions of self-assessment*. OUP Oxford, Oxford, 1985.
[139] F. Teroni and J. A. Deonna. Differentiating shame from guilt. *Consciousness and Cognition*, 17(3):725–740, 2008.
[140] A. Tims. Haunted by shame: victims of bank transfer scams tell of lasting trauma, 2021. Retrieved 18 April 2021 from: https://www.theguardian.com/money/2021/apr/17/bank-transfer-scams-fraud-victims.
[141] J. L. Tracy and R. W. Robins. Putting the Self Into Self-Conscious Emotions: A Theoretical Model. *Psychological Inquiry*, 15(2):103–125, 2004.
[142] L. K. Treviño, G. R. Weaver, and S. J. Reynolds. Behavioral ethics in organizations: A review. *Journal of Management*, 32(6):951–990, 2006.
[143] P. Twomey. How Should We Tackle the Challenges of Today's Cyber Security Environment?, 2017. Centre for International Governance Innovation. Retrieved 30 March 2021 from: https://www.jstor.org/stable/pdf/resrep05241.9.pdf.
[144] P. Velotti, J. Elison, and C. Garofalo. Shame and aggression: Different trajectories and implications. *Aggression and Violent Behavior*, 19(4):454–461, 2014.
[145] W. Verbeke and R. P. Bagozzi. A situational analysis on how salespeople experience and cope with shame and embarrassment. *Psychology & Marketing*, 19(9):713–741, 2002.
[146] J. Wailes-Fairbairn. Cyber shame: how to avoid the stigma of being a victim, 2020. Smart Security. Smart Compliance. Retrieved 24 May 2021 from: https://www.srm-solutions.com/blog/cyber-shame-victim/.
[147] Y. Wang. Lingering guilt and shame: Emotional burdens upon those who intended but failed to apologize. *The Journal of Social Psychology*, 160(5):675–687, 2020.
[148] M. Wenzel, L. Woodyatt, and B. McLean. The effects of moral/social identity threats and affirmations on psychological defensiveness following wrongdoing. *British Journal of Social Psychology*, 59(4):1062–1081, 2020.
[149] M. T. Whitty and T. Buchanan. The online dating romance scam: The psychological impact on victims–both financial and non-financial. *Criminology & Criminal Justice*, 16(2):176–194, 2016.
[150] A. C. Williams, G. Mark, K. Milland, E. Lank, and E. Law. The perpetual work life of crowdworkers: How tooling practices increase fragmentation in crowdwork. *Proceedings of the ACM on Human-Computer Interaction*, 3(CSCW):1–28, 2019.
[151] B. Wittes, C. Poplin, Q. Jurecic, and C. Spera. Sextortion: Cybersecurity, teenagers, and remote sexual assault, 2016. Center for Technology at Brookings. Retrieved 24 May 2021 from: https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf.
[152] Y. Wong and J. Tsai. Cultural models of shame and guilt. In J. L. Tracy, R. W. Robins, and J. P. Tangney, editors, *The Self-Conscious Emotions: Theory and Research*, page 209–223. Guilford Press, New York, USA, 2007.
[153] J. V. Wood, M. Giordano-Beech, K. L. Taylor, J. L. Michela, and V. Gaus. Strategies of social comparison among people with low self-esteem: Self-protection and self-enhancement. *Journal of Personality and Social Psychology*, 67(4):713–31, 1994.
[154] F. Wright, J. O'Leary, and J. Balkin. Shame, guilt, narcissism, and depression: Correlates and sex differences. *Psychoanalytic Psychology*, 6(2):217–230, 1989.
[155] L. Xing, J. J. Sun, and D. Jepsen. Feeling Shame in the Workplace: Examining Negative Feedback as an Antecedent and Performance and Well-Being as Consequences. *Journal of Organizational Behavior*, 2021. In press. https://doi.org/10.1002/job.2553.
[156] Z. Xu and H. Guo. A meta-analysis of the effectiveness of guilt on health-related attitudes and intentions. *Health Communication*, 33(5):519–525, 2018.
[157] D. Zahavi. *Self and other: Exploring subjectivity, empathy, and shame*. Oxford University Press, Oxford, UK, 2014.
[158] M. Zec. Cyber security Measures in SME's: a study of IT professionals' organizational cyber security awareness. Master's thesis, Information Systems, Linnaeus University, Kalmar, 2015. http://www.divaportal.org/smash/get/diva2.
[159] J. Zhuang. *Are guilt and shame distinguishable?–Exploring persuasive effects of guilt and shame on information processing from two novel dimensions*. PhD thesis, Communication, Michigan State University, 2014.
[160] V. Zimmermann and K. Renaud. Moving from a 'human-as-problem" to a 'human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, 131:169–187, 2019.
[161] P. R. Zuzelo. Smokers' guilt and shame: Reactions to smoking and to providers' cessation efforts. *Holistic Nursing Practice*, 31(5):353–355, 2017.

A SURVEY QUESTIONS

A.1 CYBER SECURITY EVENT HAPPENED TO YOU

The following questions seek to elicit information about being involved in cyber security events.

Think about a time in the past when you experienced an adverse phishing or cybersecurity event at work, e.g., you fell for the Phish or lost data or your device (or your employer's) was compromised.

Can you recall such an event? (Y/N)

Please try to recall the event in as much detail as you can. Try to remember your thoughts and feelings at the time.

How did you feel at the time? (You're anonymous, so feel free to be frank and open - we don't judge)

Was anyone else involved in the event?
If yes:

- Please explain about how the other person was involved
- Did they have the same response from others as you? If not, what was different?
- Was the final outcome the same as yours? Or different? Tell us more.

A.2 HAPPENED TO SOMEONE ELSE

Someone might have told you about an incident when they experienced an adverse phishing or cybersecurity event, e.g., they fell for a Phish or lost data or their (or their employer's) device was compromised. Can you recall someone telling you about such an event?

- Yes, it happened at work (or while they were working from home during the pandemic)
- Yes, it happened at home (in their personal capacity)
- No, I don't remember anyone telling about an event like this

If yes,

- How did they feel about what happened? Try to remember what they told you about their thoughts and feelings at the time.
- Please try to recall the event in as much detail as you can. How did their employer handle the event?
- How did they feel about their employer after the event?

A.3 DEMOGRAPHICS

- Gender
- Education
- Ethnicity
- Age range