Cybersecurity Regrets: I've had a few .... *Je Ne Regrette*

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

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

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

ABSTRACT

James Baldwin says: "*though we would like to live without regrets, and sometimes proudly insist that we have none, this is not really possible, if only because we are mortal*". The field of cybersecurity has its fair share of poor outcomes, some of which are bound to be due to regrettable actions. Similar to other negative emotions, such as fear and shame, it is likely that organisations are using anticipated regret as a behavioural control mechanism in the cybersecurity domain. We explore the nature and characteristics of cyber-related regrets, and the extent to which regret (both anticipated and experienced) influences future cybersecurity decisions. We derive a process model of regret and report on the way cybersecurity regrets occur, what their outcomes are, and how people experience them. We conclude with suggested directions for future research.

CCS CONCEPTS

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

KEYWORDS

regret, cybersecurity, regret appeals

ACM Reference Format:
Karen Renaud, Marc Dupuis, and Rosalind Searle. 2022. Cybersecurity Regrets: I've had a few .... *Je Ne Regrette*. In *Proceedings of 2022 New Security Paradigms Workshop (NSPW '22).* ACM, New York, NY, USA, 20 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

> *"Dear as remember'd kisses after death,*
> *And sweet as those by hopeless fancy feign'd*
> *On lips that are for others; deep as love,*
> *Deep as first love, and wild with all regret;*
> *O Death in Life, the days that are no more!"*
> The Princess: Tears, Idle Tears by Alfred, Lord Tennyson

NSPW '22, October 24–27, 2022, New Hampshire
© 2022 Association for Computing Machinery.
ACM ISBN 000…$15.00
https://doi.org/10.1145/nnnnnnn.nnnnnnn

1 INTRODUCTION

Hampshire [40] suggests that regret is a fact of life, felt when a poor decision leads to an unfavourable outcome. Cybersecurity is infused with decision making, and poor outcomes are common. Consider the chief security officer of a college that experiences a ransomware attack, only to realise that their backup strategy was inadequate [62], the person who is deceived by a Phishing message [4], or the person who accidentally and permanently deletes valuable records [37]. All are bound to feel regret because their initial decisions led to adverse and unintended outcomes.

Regret is seen as a negative emotion [133], which manifests as an intensely personal emotional experience [57]. It also has a cognitive dimension [59], which leads those with regrets to ruminate about what 'might have been' if decisions had been different. Regret can have both positive [75] and negative [87] outcomes.

Festinger [27] argues that when people feel regret, they attempt to revoke the decision psychologically. He suggests that when a person realises that the outcome is not as anticipated, their mind immediately starts focusing on the attractiveness of the not-taken option.

Kahneman and Tversky [51] call regret a *counterfactual* emotion, an appropriately descriptive term to reflect its cognitive dimension. Most importantly, such counterfactual thinking has the potential to alter future behaviour [86]. Regret, it is argued, makes it possible for people to learn from their mistakes. Indeed, Saffrey *et al.* 's [92] studies found that people actually valued their regrets, which provided them with insights, promoting psychological growth and helping them learn from their mistakes. However, regret can also lead to excessive rumination, and consequent depression and anxiety [87].

Connolly and Zeelenberg [15] explain that the emotional side of decision making is important. Knowing this, organisations sometimes use negative emotions as behavioural control mechanisms in the cyber domain [82, 83]. It is likely that organisations use anticipated regret as they use other negative emotions, but this particular emotion does not appear to have received much research attention in the cyber domain[1]. Roese *et al.* [90] argue that the regret emotion is pivotal for decision making and should be studied in the context of behaviour regulation. As such, in this paper we examine the experiences of regret during cyber decision making and the consequences of experienced regret.

This paper's title reflects our findings: some experience cybersecurity regrets and learn from them ('I've had a few' from Frank Sinatra's famous song: *My Way*). Others do not regret particular events, and thus do not learn from them (*'Je Ne Regrette'* sung by the great Edith Piaf). Whether employees learn from regrets or not

[1] a search for "regret-appeals" & cybersecurity in April 2022 returned only one paper

depends on the organisation's own supportive and conscientious cybersecurity behaviours.

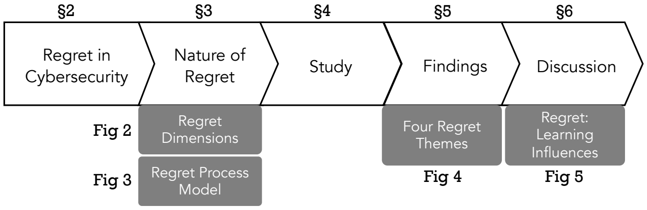

Figure 1: Structure of this Paper

As shown in Figure 1, we commence by reviewing research that has addressed regret in the context of cybersecurity in Section 2. We then explore the nature of regret in Section 3, and outline the details of the study we carried out to explore the prevalence and influence of regret in cybersecurity in Section 4. Section 5 presents our findings, which we discuss in Section 6. We conclude in Section 7. The contributions of this study are:

- From the research literature:
  - Regret dimensions (Figure 2).
  - A regret process model (Figure 3).
- From the survey:
  - Four cybersecurity regret themes (Figure 4).
  - Factors that encourage learning from cyber regrets, and those that discourage it (Figure 5).
  - Research and practical implications and suggestions for future work (Section 6).

2 REGRET IN CYBERSECURITY

Regret has not received much attention in the cybersecurity domain, with some notable exceptions [71, 117, 118]. We should also note, at this point, that cybersecurity and privacy are distinct and different constructs and we will only be dealing with the former in this paper, acknowledging that privacy decisions, too, deserve investigation in this respect.

Use by governments: We first consider national awareness drives to explore governments' use of anticipated regret in their campaigns. Van Steen *et al.* [115] reviewed behaviour change techniques deployed by government-led cybsersecurity awareness campaigns. They report that Hong Kong's Cyber Security Information Portal[2], Nigeria's National Cyber Security Awareness Month (NCSAM) campaign (2012-2014)[3], and the USA's Stop, Think, Connect campaign[4] all used regret appeals in their awareness campaigns. The authors do not report on the efficacy of these campaigns, so perhaps the governments are not releasing this evidence.

Evidence from regret studies: Wisniewski *et al.* [124] explain that people reflect on past behaviours when deciding to share their location on their Smartphones. They argue that people learn from regrets arising from their prior privacy-related decisions. Wright and Ayton [126] showed that regret messages encouraged users to back-up their data. However, it did not influence their web-surfing activities, particularly behaving securely. In the context of identity theft, Ogbanufe and Pavur [71] revealed anticipated regret was associated with adaptive coping responses, as is response efficacy.

Moreover, self-efficacy and anticipated regret were associated with Smartphone security intentions. Anticipated regret and prior intentions positively influence behaviours. Moreover, Verkijika [118] subsequently showed that anticipated regret exerted a positive influence on mobile phishing avoidance motivation and behaviours.

The experience of regret can help to neutralise the endowment effect [65], which Renaud *et al.* [82] showed prevented people from changing the way they create their passwords. The obvious question to ask is whether deactivating the endowment effect would be a strong enough motivation for using of regret appeals in the cyber domain.

Theories: Protection motivation theory [109] and theory of planned behaviour [104] are widely used to model behaviour in cybersecurity research. It is interesting that Verkijika [117] integrated anticipated regret into their Protection Motivation Theory model, to discover that perceived vulnerability and severity significantly influenced anticipated regret. Furthermore, Sommestad *et al.* [104] argue for the addition of anticipated regret to the theory of planned behaviour, enhancing intentions to comply with security policies.

What happens after regrettable outcomes? In the aftermath of adverse cybersecurity events, how the organisation handles the situation can have long-term consequences [83]. Given that Van Kleef *et al.* [114] showed how emotional expressions could trigger affective reactions in others, and Kox *et al.* [58] found expressed regret could repair trust, an expression of regret from someone who triggers an adverse cyber incident has the potential to placate managers.

Before outlining our study, we first examine the nature of regret in the next section.

3 THE NATURE OF REGRET

Landman [59, p. 145] defines regret as '*being sorry for losses, mistakes, or other events*'. It is important to note that in this definition there is no suggestion of wrongdoing. Rather, it alludes to: (1) the negative emotion of sorrow, and (2) an undesired outcome (losses), and mistakes being made. Inherent to more intense regret is the rumination that arises from the lack of closure and ongoing meaning-making which can fixate on a lost desired potential self and goals that the undesirable outcome has rendered irretrievable. This might lead to diminished self-esteem and reduction in future options [5]. There can be a grieving for this lost opportunity [89].

There is a suggestion of self-reflection of a shortcoming accompanied by negative emotion (sorrow). d'Avelar's [24] characterisation of regret suggests that this definition is lacking, because it does not incorporate regret's social [107] and cultural dimensions [20]. We will thus consider all aspects of regret before reporting on our empirical investigation.

3.1 Regret Dimensions

Regret has a temporal nature. Landman [59] reflects that regret can occur for events that may have occurred in the past, the present or future. In terms of the future, the person might be required to do something they regret, such as firing someone, but this does not

[2] https://www.cybersecurity.hk/en/index.php
[3] https://www.ncsam.com.ng
[4] https://www.stopthinkconnect.org/contact

involve any decision making which they can regret on a personal level.

Williams [123] differentiates between two forms of regret: agentic and impersonal. *Agentic* is related to something the individual did and did not do, that led to less than desirable outcomes. *Impersonal* regret, by contrast, is related to something that might have happened, but which the individual had no hand in. An example of the first is clicking on a Phishing message, while the latter occurs when an organisation experiences a data breach regretted by all employees, even though they have no responsibility for securing the organisation's systems.

Wallace contends that regret can arise from either accidental or deliberate actions [119]. An individual may feel regret even if they did not intend something to happen – anyone who has accidentally dropped and broken something has felt such regret. Regret is the cognitive and emotional response to their self-reflection of the shortcoming and incurred loss [89].

Finally, Landman [59] explains that regret can result from sins of commission (action regret) or of omission (inaction regret). Figure 2 depicts all the dimensions we have mentioned in this section.

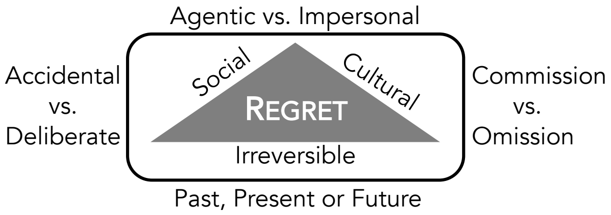

Figure 2: Regret's Dimensions

Our focus, in this paper, is on agentic regret related to intentional actions, and the role of regret in meaning- and decision-making.

3.2 Regret Process Model

Gilovich and Medvec [31] argue that there is a temporal pattern to the experience of regret. Hence, it is helpful to construct a process model of regret in order to understand how regret works.

A process model depicts pathways that people can take from a starting point to an ending point. When referring to regret, this commences with a decision making stage, and ends with experienced regret. The model is not causative, rather seeking to demonstrate the complexity of the emotion and the differences in how people might experience it.

Regret Stages:

Connolly and Reb [14] argue that the *choice itself*, the *process* of making the choice, and the *outcome* should be considered as core parts of regret. The first two of these could fit into a 'decision making' stage, with the third being the act of comparing desired to expected outcomes: an 'action & appraisal' stage.

Sugden [106] suggests two stages: (1) the desire that a decision could have been made differently, and (2) self-recrimination and self-blame for that choice. These both seem to be actions that occur after the two stages outlined above, what we will call the 'experienced regret' stage.

Connolly and Zeelenberg [15] propose Decision Justification Theory (DJT), which has two core components: (1) a comparative evaluation of the outcome, and (2) blaming one-self for having made a poor choice. The first of these aligns well with the 'action & appraisal' stage, while the third aligns with the 'experienced regret' stage.

The last stage, once regret has been felt, will often entail counterfactual thinking [51], which would likely incorporate Sugden's first and second components. There would also be a measure of sense-making, and sometimes long-term consequences of the experienced regret if people cannot move on.

We will use the three identified regret stages to structure the process model: *first*, making the decision [14], *second*, acting & appraising the outcome [15], and *third*, experienced regret [106]).

Developing the Process Model: As we present the components of the process model, numbered references e.g., *cmp i* refer to components (states or decision points) of Figure 3 and *S i* refers to stages 1, 2 or 3. We will also review individual moderators of the process after discussing the three stages.

(Stage 1) Decision Making.

Decision making is difficult in conditions of uncertainty [50] or too much choice [48]. Lin *et al.* [61] and Connolly and Reb [14] refer to the decision making stage as a *mental simulation of outcomes*. This kind of anticipation will only be part of the decision making process where it is not possible for the person to predict the outcome – where they simply cannot know how things will pan out. Moreover, it suggests that the decision maker has the capacity to conceive multiple alternative outcomes [40] (cmp9).

Sugden [106] suggests that individuals who are engaged in decision making will anticipate regret (cmp2) or rejoicing (cmp1) as the outcome of their decision. Indeed, Bjälkebring *et al.* [9] confirm that regulation and prevention of regret influences decisions. Zeelenberg [128] found that anticipation of future regret, as well as experiences of previous regretting experiences (cmp3), would influence behaviour, confirmed by [16, 42, 96]. Hayes [42] contended that this would assist people to learn from their mistakes, which Wong and Kwong's [125] study confirmed (S3 → cmp3). Lin *et al.* [61] found that the impact of previously experienced regret on future decisions was dependent on risk levels. If the decision is low risk, experienced risk had a lower impact than if the decision was high risk (cmp3 → cmp2).

Zeelenberg *et al.* [131] showed that anticipated regret could force decision makers towards regret-minimising options (cmp6). They argue that people can be regret-averse, confirmed by [25, 49], perhaps in the same way as they can be shame-averse [83]. Reb [80] suggests that regret aversion leads to better decisions, because it makes people more careful in their decision making. Gilbert *et al.* [29] suggests that the dread people have for experienced regret may be unrealistic, as their actual regret will not be as hard to deal with as they anticipate.

Regret aversion also has social dimensions (cmp5 → cmp6). Van der Schalk *et al.* [112] found that social appraisals would influence decisions, and that this may contribute to maintenance of social norms. However, Summerville and Buchanan [107] contend that social expressions of regret are different from private experiences in both their form and function. They outline how private experiences include making causal connections and learning (cmp8), while social expressions of regret can facilitate social cohesion through indicating awareness of error and contrition for actions, that could be viewed as an apology. In an interesting study into students' experiences of regret following binge drinking events, Crawford *et al.* [17] find that students prioritise participation in such events, and feel that missing out on these would lead to greater regrets than regrets related to hangovers that result from participation (cmp5 → cmp2).

(Stage 2) Action & Appraisal.

Having made a decision,arriving at a choice in the previous stage, this choice is carried out: either in acting or abstaining from acting (cmp7 → cmp10 & cmp11).

The actual outcome of the choice (cmp12) will be observed, and compared (cmp13) to the expected outcome (cmp9). If these match, the individual is satisfied (cmp13 → satisfaction), and regret does not occur. If not, there are a number of options resulting from the appraisal [67]: (1) anger at oneself (cmp14), (2) anger at circumstances (cmp15), (3) disappointment (cmp13 → disappointment), and (4) regret (cmp13 → S3).

(Stage 3) Experienced Regret.

The experienced regret stage has some sub-stage. It is likely to involve a counterfactual sub-stage [51]. The second sub-stage occurs as the person attempts to make sense of what has happened, and the third entails the long term consequences of the regret. Finally, there is a potential link from this experienced regret to future decisions.

(3a) Counterfactual Thinking: Harking back to Kahneman and Tversky's [51] nomenclature: regret is a counterfactual emotion. Pink [76] refers to counterfactual thinking as "*the human ability to mentally travel through time and conjure incidents and outcomes that never happened*" i.e. concocting events that run counter to the incontrovertible facts. Regret-related counterfactual thinking includes self-reflection, where the actual outcome is contemplated (cmp16), the choice process evaluated (cmp17) and the choice itself second guessed (cmp18). This leads to self-appraisal [51] (cmp20).

Counterfactual thoughts refer to thoughts at odds with the facts [26]. There are two mechanisms to this kind of thinking: (1) contrast effects, and (2) causal inference effects. Contrast effects compare the outcome to some personal anchor so that the same outcome might be appraised differently by two people due to their different anchors. With the latter mechanism, the person attempts to make sense of the undesirable context, and may include blaming (cmp20) and an overconfidence in their explanations of the outcome (cmp26). Such thinking has an important role, informing decisions, and placing knowledge into context [88] (S3 → cmp3). Roese and Morrison [88] explain that counterfactual thinking can, in fact, be persuasive and entertaining.

Tsiros and Mittal [110] find that people are most likely to generate counterfactuals when the expected outcome is negative and different from the status quo (cmp13 → cmp 16, 17 & 18). Pink [76], however, points out that counterfactual thinking seldom makes people feel better about what happened. Indeed, he contends that the purpose of this thinking is to make people feel worse because that drives them to do better in the future (cmp3).

(3b) Sense Making: Price [79] argues that regret is "*is a feeling that brings us back to reason*" (p. 4). Any hot emotions, such as anger [7] can skew the types of information and memories recalled and can lead people to act unwisely. The incident would now be cognitively processed, ruminated over, and will inform subsequent decisions (S3 → cmp3). Roese *et al.* [87] discovered an association between regret and what they call 'repetitive thought' (the rumination that [134] refer to) (cmp19). They also found that regret could lead to depression and anxiety (cmp24) and possible grieving (cmp25).

Zeelenberg *et al.* [132] find that decisions to act produce more regret than decisions to abstain from acting – something they term the "*inaction effect*". Landman [59, p. 139] cite a number of studies that confirm this bias. There is a general tendency to action [3], which might colour the tendency for regret. However, Gilovich and Medvec [30] report that whereas regretted actions would indeed be more painful in the short term, it was inaction that led to greater regret in the long run (cmp10 → cmp19). Gilovich *et al.* [32] found that action-related regrets were related to 'hot' emotions (cmp7 → cmp11), while inaction regrets were more related to wistfulness or despair. Moreover, the authors argue that inaction regrets are more troublesome because they linger longer.

(3c) Coping: Gilbert *et al.* [29] showed that people feel more regret when the choice they made was almost the right decision, leading to a sense that more could have been done (cmp23).

Finally, Van Dijk and Zeelenberg [113] discovered that as people process the feelings of regret, they might try to identify compensatory silver linings (cmp22) in order to better cope with the situation; It offers a more palatable alternative, to counterfactual thinking.

(3d) Long Term Consequences: Beike *et al.* [5] report that people feel greatest regret for outcomes where their wrong choice represents a lost opportunity (cmp23), with no way available to change things in the future. They cited career, education and romance as three areas where such losses feel final. This perspective was confirmed by Effron [25]. Roese and Summerville [89] suggest that people's biggest regrets tend to be related to areas where they have perhaps not embraced opportunities for change, growth and renewal (cmp14, cmp15 → cmp19).

Influencing Future Decisions: Sijtsema *et al.* [98] found that regret, when paired with high levels of self-regulatory abilities, could indeed be a salutary experience (S3 → cmp3), while for those with low self-regulatory abilities, it could lead to ruminative brooding (cmp23).

Individual Moderators

Hart *et al.* [41] found that a belief in a deity and divine control appears to reduce their counterfactual thinking [63].

Kamiya *et al.* [53] argue for two kinds of decision makers: maximisers and satisficers. They suggest that maximisers are taught to decrease their goal in order to ensure that they can cope with regret more effectively, while satisficers' propensity for "good enough" decisions, means they do not benefit from such goal reduction, because they are less prone to excessive levels of regret (cmp22, cmp26).

De Groot *et al.* [20] found that those from collectivist cultures have different regret experiences than those from individualistic cultures, confirming the social dimension of regret experiences also reported by [107, 112] (cmp8). This means that even if the same outcome is seen as equally undesirable by two different individuals, they may experience it differently. For example, Heine and Lehman [44] revealed how Japanese participants experience greater self discrepancies than Canadians, while Breugelmans *et al.* [11] found that Taiwanese participants felt more intense emotions of regret and guilt than American participants in the same experiment.

The literature is clear about the fact that some people have a greater risk appetite than others [74, 120], and we also know that an effect called 'risk homeostasis' is believed to moderate risky behaviours [84]. This particular propensity is encapsulated within cmp6 in the process model. We also have to acknowledge the fact that reference levels are individualistic. Each person's individual position is an important reference point [6]. What is disappointing for one person may be seen as a perfectly acceptable outcome for another (cmp9 → cmp12).

***Summary*.**
Figure 3 depicts the regret process from initial decision making thought processes to regret processing and consequences. We now compare regret to other emotions that it is commonly conflated with.

3.3 Comparisons with other Emotions

In order to understand regret in this context, it is helpful to differentiate it from other emotions. We searched for publications that compared regret to other emotions and explain how these fit into the process model.

Extant study considers regret to be distinct from other emotions found in moral dilemmas, where it is important for decision-making, elicited as part of the comparison of a variety of potential choices [77]. Although moral violations are also noted to elicit guilt, shame, anger and disgust, regret is most significant in terms of decision making. Research shows that basic moral emotions of anger and disgust can arise as a result of breaches of moral codes, and that they produce distinct cognitive responses: notably, hostility and engagement from anger, and withdrawal from disgust [33]. Critical to this paper and its focus on cyber security, disgust triggers avoidance with a lack of engagement as to *why* this is the case, while anger produces immediate responses which are then a source of subsequent remorse and regret. Here, we will focus on a nominological set of emotions that are more typical in the cybersecurity context.

***Regret vs. Guilt*.**
Lewis [60] explains that both regret and guilt involve self-awareness, and of how one has fallen short. Self-reported ratings of the two reveals their high correlation [64], and similar ways people cope with these emotions [103]. Yet, regret and guilt are indeed different emotions [8]. Turner and Underhill [111] explain that guilt arises when there is harm to others, and not only to one-self, citing [129].

Zhang *et al.* [135] suggest that we can distinguish these emotions by examining their connections with people's perceptions of their own self discrepancies. Higgins [46] explains that self-discrepancies occur for two reasons: first, when we compare ourselves with our personal "*ideal self*", and second, when we compare ourselves with our "*ought self*" (cmp13 → Guilt). Zhang *et al.* [135] conclude from their investigation that regret is experienced when people feel they have not lived up to their 'ideal' self. Renaud *et al.* [83] consider that shame occurs under the selfsame differences where there is a perceived discrepancy between ideal self and actual self. It might be that shame and regret are experienced at the same time when this happens.

Zeelenberg and Breugelmans [129] revealed another difference between the two, with guilt generally arising when others have been harmed, whereas regret is felt both when others and the person him or herself has been harmed by the events. Hence, guilt is reflected in the process model as emerging from cmp13 when the person realises that harm has been caused to others.

An example from the cybersecurity domain is highlighted by Kempen [55]. A municipal employee violated policies by installing software on his work computer. The software captured his credentials by logging keystrokes, giving criminals access to the municipality's bank account. The municipality lost a great deal of money. When municipalities lose money, they will not be able to deliver the full range of services to their communities. Hence, all residents were potentially harmed. In this situation, it is likely that he felt guilt.

Another example comes from the Target data breach that occurred in 2013. A third-party contractor, Fazio Mechanical Services, is believed to have fallen victim to a phishing attack [97]. This resulted in the eventual installation of malware. The problem stems from the access that Fazio Mechanical Services had to Target. As a contractor, they had access to Target's external billing system, Ariba. Given the lack of network segmentation on Target's networks and the access the malicious actors now had to Fazio Mechanical Services computers, the malicious actors were eventually able to place malware onto Target's POS (point of sale) system. This resulted in the theft of approximately 40 million credit card numbers and over 70 million personal records. The harm that was caused to so many others, and not necessarily to the individual from Fazio Mechanical Services that originally fell for that phishing email, likely resulted in significant guilt on the part of this individual.

***Regret vs. Disappointment*.**
Both these emotions are related to an undesirable outcome [134]. Zeelenberg *et al.* noted significant divergence between the two with respect to their implications for future behaviours. Regret, they found, was related to a feeling that the person ought to have known better, accompanied by a strong desire to correct their initial mistake. Disappointment, on the other hand, left the person wanting to move on from the powerlessness they felt over the situation and an outcome they feel responsible for. They explain that those who regret have a tendency to ruminate, re-playing the initial event, while those experiencing disappointment were able to move on more easily.

Van Dijk and Zeelenberg [113] suggests that when a decision leads to an undesirable outcome, disappointment occurs if a better outcome was expected. Regret, however, occurs when there is a sense that a better outcome could have occurred if only the person

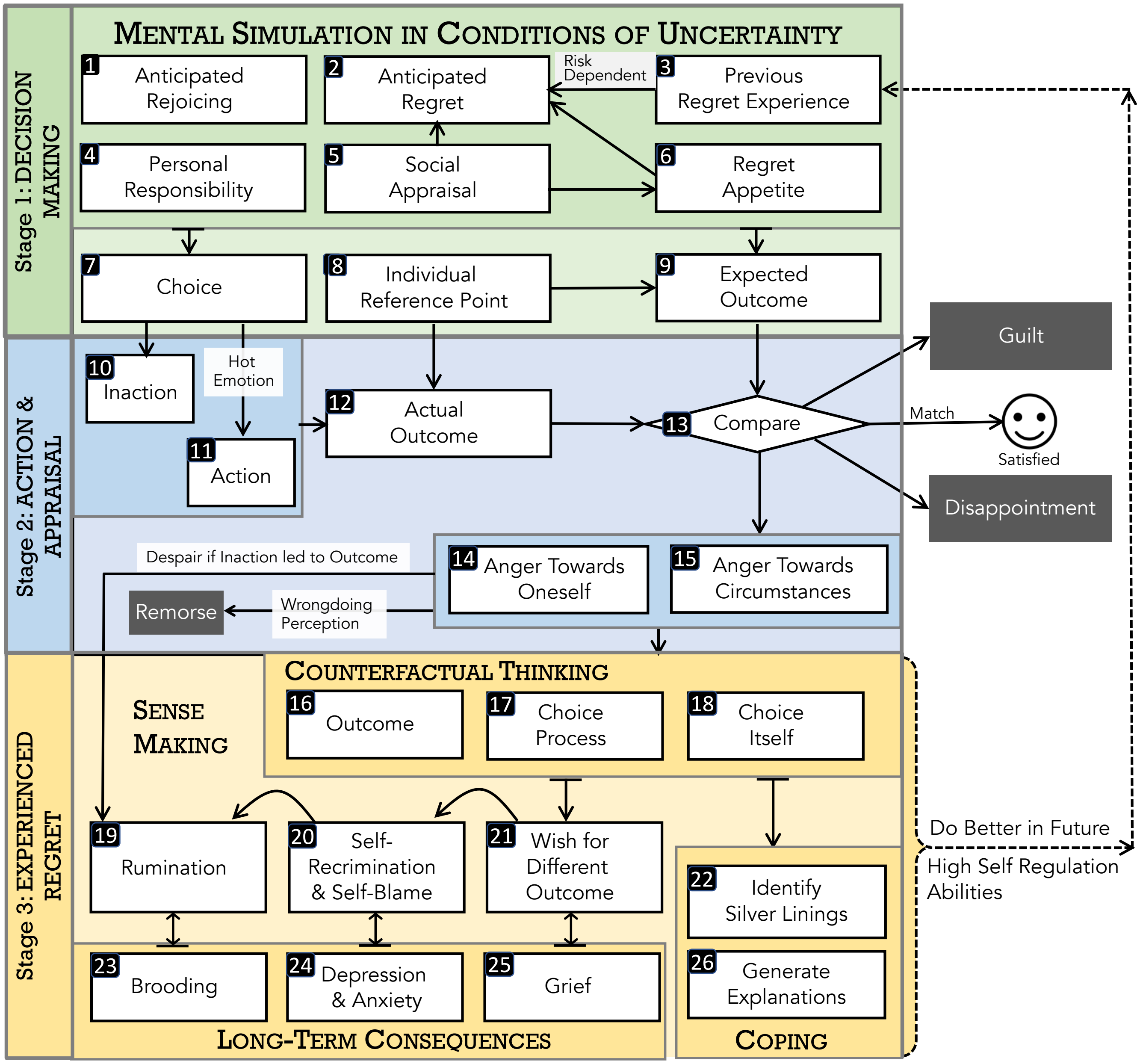

Figure 3: Agentic Regret Process Model (rectangles are components, diamonds a decision point, arrows reflect state transitions, dark rectangles are other emotions that we compare to regret)

had chosen differently. Thus, it is the loss of a potentially better current and future outcome.

Interestingly, Zeelenberg and Pieters [130] found that those who experienced disappointment were more likely to share their experiences with those in their social network, whereas regretters were likely to keep it to themselves. However, those who regretted were more inclined to act based on their experiences, altering their future actions, as compared to those who experienced disappointment.

Hence, disappointment emerges from cmp13 when the outcome has been out of the person's control i.e., not as a consequence of a personal bad decision. An example here occurred when T-Mobile was hacked, again, in 2021[5]. While T-Mobile customers did choose to sign up, they could not have foreseen the negative outcomes of their decisions.

[5] https://malimar.com/2022/05/02/the-experian-hack-one-of-the-biggest-modern-data-breaches/

Similarly, in the United States many individuals undergo federal background checks when entering a position of trust and with potential access to classified material [35]. This includes governmental personnel, military personnel, and federal contractors, among others. In 2015, the Office of Personnel Management (OPM) suffered a significant data breach in which over 21 million federal employees background information was stolen. As a condition of employment, individuals are required to provide the information necessary for the background checks to be completed. They did not have a choice in providing that information, nor were they in a position to protect that information once provided. In the aftermath of the OPM data breach, it would be understandable if many of the victims of this data breach felt significant disappointment. There were not any components of the data breach that the average victim would likely regret, *per se*, given their inability to have made a different decision that would have resulted in a different outcome. Instead, a sense of powerlessness was likely felt by these victims with significant disappointment in an outcome over which they had no control.

Regret vs. Remorse.

Another similar emotion is remorse, which is defined by Landman [59] as "*a gnawing distress arising from a sense of guilt for past wrongs*". Landman [59] contrasts regret and remorse, explaining that remorse is related to a sense of guilt concerning a prior wrongdoing. These two emotions are connected as both involve pain and distress (citing [102]). Yet, one study, by Russell and Mehrabian [91], found that remorse was less unpleasant than regret. This increased unpleasantness associated with regret seems to arise from the intrusive recall of events and associated negative emotions (sorrow) [5].

A further difference concerns their antecedents, with moral wrongdoing preceding remorse, while regret does not require this antecedent. Thus, one may *regret* not being able to attend a funeral, and feel *remorseful* about treating that person badly when they were alive.

Landman [59] outlines defining features of their divergence, with remorse producing an intention not to commit the same act again in the future, which is sometimes absent from regret. She concludes that remorse entails a measure of personal responsibility, that is not always a feature of regret. Moreover, regret may be linked to attitudes - perhaps previously held biases towards minority groups - even if not acted upon. Remorse, on the other hand, is inextricably linked to moral wrongdoing or a failure to act. Finally, while people may feel both regret and remorse for an action, if their action is immoral, remorse would be the more salient emotion. Hence, remorse arises from components cmp10 and cmp11 if there is a recognition of wrongdoing having being engaged in.

An example occurred when a British hacker compromised companies, stole their data and sold it on the dark web [108]. The report says that he expressed remorse for what he had done and the people he hurt with his actions.

Additionally, we often hear of the insider threat within organisational settings, whether malicious or non-malicious in nature [22]. A malicious insider often acts in a manner devoid of moral or ethical concern [39], whereas a non-malicious insider may unintentionally cause damage to an information system [22]. Thus, if a non-malicious insider used the organisation's information systems to make a personal purchase on a website and this resulted in the unintentional installation of malware, the employee would likely feel some level of remorse for the decisions made that resulted in this outcome, especially given the questionable ethics and morals behind that decision.

3.4 Wielding Emotions

Organisations sometimes deliberately use emotions to encourage compliance, for example in their use of fear appeals [81] and shame [83]. Advertising often deploys guilt appeals [47]. Huhmann and Brotherton [47] explain how shame appeals can trigger purchases to avoid disgrace, while fear appeal responses involve attempts to re-establish perceived control. In contrast, a guilt appeal triggers a purchase designed to assuage guilt, and a regret appeal utilises dissatisfaction from prior purchases leading the acquisition of the advertised product to reduce anticipated future feelings of regret. Making anticipated regret salient has conceptually [99] and empirically [12, 93] been shown to effect purchase decisions.

Empirical Studies: Simonson [99] found that anticipated regret influenced people's purchasing decisions. Regret appeals have proven efficacious in the health domain [66] encouraging young women to take Folic Acid. Furthermore, Kajzer *et al.* [52] found those high in agreeableness would be more likely to respond to regret-based awareness campaigns.

Where organisations deliberately trigger feelings of anticipated regret, their intention is to produce compliance with organisational policies. In this endeavour, regret needs to be made salient [72], because people do not always spontaneously anticipate regret that might have stemmed from their previous actions or inaction [18].

Certainly, there is evidence from marketing that shows that regret appeals can have desired effects. For example, Hetts *et al.* [45] found regret salience influenced precautionary behaviour uptake, while Passyn [72] showed adding regret to fear appeals enhanced their effectiveness. In the health domain, and making anticipated regret more salient encouraged people to take more exercise [2].

Unanticipated Side Effects: Crawford *et al.* [18] revealed that explicitly asking people to anticipate regret could also lead to 'mis-anticipation' of their future feelings. In an interesting comparison between fact-, fear- and regret appeals, Grasshof *et al.* [36] found that while regret appeals influenced action-related coping with the threat, fear led to denial coping. Those receiving fact-related appeals coped in line with their own individual threat coping style. Smerecnika and Ruiter [101] showed anticipated regret was a qualified mediator of fear appeal message from its intention. Others have demonstrated that coping appraisals (response efficacy) are more predictive of taking protective action than threat perceptions (i.e. fear appeals) [28, 34]. Moreover, Smerecnika and Ruiter [101] contend fear can inhibit the motivation to engage in fear-control processes instead of choosing danger-control actions. Finally, fear can escalate denial and flight responses [69, 73], whereas regret is forward-looking [94], offering the opportunities to do better in the future.

Challenges: It is difficult to calibrate the extent of the negative emotion that an appeal can trigger, or the other emotions that arise, and the long-term consequences of these appeals [23].

Summary: Now that we understand the nature of regret, we can outline our study, which seeks to determine the potential consequences of regret in the cybersecurity domain.

4 STUDY

Drawing on extant literature, this study explores regret in the context of cybersecurity, to investigate the following questions :

RQ1: What *characterises* regrets felt by people in the cybersecurity domain? (which emerged from Sections 2 & 3)

RQ2: How does *anticipated* regret influence cybersecurity decision making? (which emerged from Section 3.4)

RQ3: How does *experienced* regret influence cybersecurity decision making? (i.e., do people learn from their cybersecurity mistakes?)

We developed a online survey to help us to answer these questions (see Appendix A), inviting respondents to tell us whether they had been involved in triggering a cybersecurity event, whether they felt regret and how they experienced it.

Our focus in this study was on the role of cyber security decision making by lay people and any possible regret that may ensue rather than cyber security professionals. While cyber security professionals have regrets, they are less likely to make common cyber security-related mistakes. Additionally, the primary focus of organisations in the deployment of security education, training, and awareness campaigns is the average employee, not the individuals tasked with cyber security as their primary objective [43]. Individuals without formal knowledge and experience in cyber security are those most likely to make common mistakes and pose a risk to organisations and themselves [116].

Ethics approval was sought and obtained. The nature of the study was considered low-risk and it therefore qualified as exempt from needing a full IRB (institutional review board) review.

4.1 Recruiting

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 $2, 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 $1 to $3. MTurk workers generally provide high-quality responses to survey data when certain quality control measures are put in place [105]. In particular, in this study multiple quality control questions were used, including a manual review of textual responses. The worker qualifications we used in this study consisted of having previously completed at least 1,000 HITS (human intelligence tasks) with a 98% approval rate or higher.

The use of MTurk workers was chosen for this study because it offers several advantages, including the ability to recruit a large geographically diverse sample (within the United States) in a short amount of time with quality comparable to other recruitment techniques [105]. While financial incentives are used to compensate Turkers for their time, this is not unique to the MTurk platform. Participant compensation is routinely employed to encourage participation, recognise participants for their time, energy, and effort, and encourage a higher response rate, among other reasons [1, 38, 100]. It is also worth noting that the use of financial incentives may aid in the recruitment and retention of participants from traditionally underrepresented groups [1, 127].

In any study that is voluntary and includes informed consent, there will be something that motivates an individual to participate—an incentive of some kind [100]. The incentive for one's participation may be more altruistic in nature, but also may be egoistic as well. Nonetheless, the quality of responses from participants that are compensated monetarily versus those that are not have been shown to be comparable to one another [19]. It is possible that the use of financial incentives may result in biased enrolment in which individuals that are more likely to rely on the income from study participation enrol in the study at a higher rate than those that do not [85]. However, the converse is also true—not providing financial incentives may result in greater enrolment bias by those with greater financial means. Demand effects should also be considered, but existing evidence suggests that financial incentives do not serve as such an inducement [70]. As part of our assessment of and concern for avoiding undue inducement [85] and ensuring the compensation provided is fair, we ask participants at the end of the survey how the compensation received for their participation in this survey compared to similar tasks. Those results may be found in the next section that details the demographics of study participants. Overall, the use of the MTurk platform to recruit participants is not perfect and has many challenges, including quality challenges that will be discussed shortly, but we believe the benefits provided by using Turkers outweigh the costs.

1,054 Turkers began our survey, with 1,000 successfully passing the two automated quality control questions that were presented to them. These automated quality control questions were designed to try and identify the use of robots or other automation techniques, while not posing any significant challenges to individuals that were reading the questions [105].In particular, our focus was on helping ensure they would correctly answer the question if they were to actually read it—we had no intent to employ deception or any significant type of challenge, such as completing a mathematical equation. For example, one of the automated quality control questions used was: "Please select somewhat disagree for this question." If they took the time to read the question then they should be able to answer it correctly since the focus of the automated quality control questions was to identify automation in the answering of questions.

We then conducted an additional quality control analysis of the open-ended questions, which uncovered awkwardly worded and difficult to decipher responses. This included several duplicates, which appeared to have been due to the use of automated or manual web scraping that sought to identify possible answers to the open-ended questions. Similar to other research [83], if the responses provided were not pertinent to the questions being asked then the responses from that participant were discarded. An additional 337 responses were discarded due to this analysis. Approximately a third (104) of these responses that were discarded were due to simply not answering the open-ended questions or providing a one word response (e.g., good) despite their responses to the multiple choice question(s) indicating they had additional detail to provide.

Overall, about 27% of participants failed a quality control check, whether through automated or textual analysis means, and another 9.9% either did not answer the open-ended questions that were pertinent to earlier responses or provided one-word answers that did not answer the questions at hand. Challenges associated with using MTurk are not new, but have become more prevalent in recent years [13, 56]. 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 [13, 54, 56, 122].

From the remaining 663 responses, 500 indicated that they worked at least part-time and used a computer as a regular part of their job. Approximately 85% (N=427) of these retained participants indicated that they had personally experienced a cybersecurity incident at work and provided qualitative responses to questions about their regret experiences in relation to cybersecurity events, including details of the event, whether a different outcome could have resulted, the current impact, and what they regretted about their original decision. Given the large sample size, the sample was randomly divided into two for coding and analysis purposes. Overall, 248 survey responses were analysed concerning descriptions of a work-related experience that they regretted using open-ended questions and multiple choice responses about this experience.

4.2 Demographics:

Most of these participants identified as male (56%) with 43.7% identifying as female. They were generally well-educated (70.1% held a Bachelor degree or higher) and younger (60.3% were between 18 and 39 years old) than the population at large. Most participants were White (74.0%), followed by Asian/Pacific Islander (8.3%), Black/African American (7.2%), Hispanic (6.1%), Other/Multi-Racial (2.2%), and Native American/Alaskan Native/Indigenous (1.4%). Overall, the demographics of our participants were similar to those found in other MTurk studies with respect to age, education, and ethnicity [21]. The demographics of this sub-sample were very similar to the sample as a whole, which had 59.3% identifying as male, 69.8% holding a Bachelor degree or higher, 62.1% between the age of 18 and 39, and 73.5% identifying as White followed by Asian/Pacific Islander (6.8%).

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 to examine possible feelings, experiences, issues, and behaviour related to employees' regret of employees in an organisational setting. Respondents to our survey included a range of sectors, with science and technology the most frequent employment context (14.4%), followed by those employed in sales and marketing roles (9.1%) and finance and accounting roles (7.5%). Given exploratory nature of our data collection efforts and analysis, and the quality control concerns that are inherent in using such this crowd-sourced data collection platform, as identified previously, we are hesitant to generalise to the MTurk population as a whole, let alone the broader population. Although these MTurk workers offer a more diverse pool of participants, as compared to college students [95], they represent a unique population of individuals that have been involved in this type of work activity to earn or supplement their income.

We also employed a measure to assess the fairness of compensation provided to participants. Based on the entire retained sample of 663 participants, 77.8% of individuals indicated that they thought the compensation received was more or comparable to other projects, while 22.2% of individuals believed that more effort was required for the compensation received.

4.3 Analysis

Our analysis comprised Braun and Clarke's [10] six stage thematic analysis, involving: data familiarisation; initial code generation; thematic search and review; and defining and naming themes. Following reading and re-reading, outlines of the cyber event most regretted, and follow up question responses, we distinguished elements of regret. Our organically-devised inductive code book noted characteristics of events both experienced and anticipated. We discerned the emotions that arose, the impacts of experiences and causal elements. The latter were informed by insights into attributions that captured events' locus of causality – distinguishing those caused by the individual from those regarded as organisational in origin [121]. New codes were discussed and agreed upon in an iterative process between one of the authors and a research assistant. Areas of divergence were noted and discussed to discern if they were captured by earlier codes or were novel. This iterative process was undertaken until we were unable to identify no further novel substantive observations or linkages. Once these first-order codes were identified, the coded extracts were revisited and reviewed to construct 2nd order themes [10]. The initial themes were then discussed within the wider team for their coherence and plausibility. From these discussions, the 2nd order themes were agreed upon and aggregated dimensions labelled.

For example, in responding to the question '*what could have been done differently?*' we distinguish those who felt these events were unavoidable and therefore regret was limited; those focused externally on organisational training support with regret not something they personally felt; while others identified their regret and outlined two distinct individual actions separating risk reduction through being more cautious, as opposed to more attention and focus.

We distinguished those who had no regrets from those who did: "*It's a mistake that I won't make again*" (R238) (internal attribution and learning informing future intention). Some had learned from the event without feeling regret "*I learned a valuable lesson at someone else's expense. I don't regret it*" (R207). The resultant coding was independently checked, verified or negotiated by one of the authors and a research assistant, in terms of the interpretation and assignment to distinct categories and the broader themes. These recursive coding discussions followed participant coding, and again when the coding was completed. The discussions focused on convergence and divergence between coders enabling reviews of interpretations, analytical patterns and differences across respondents enhancing analytical credibility.

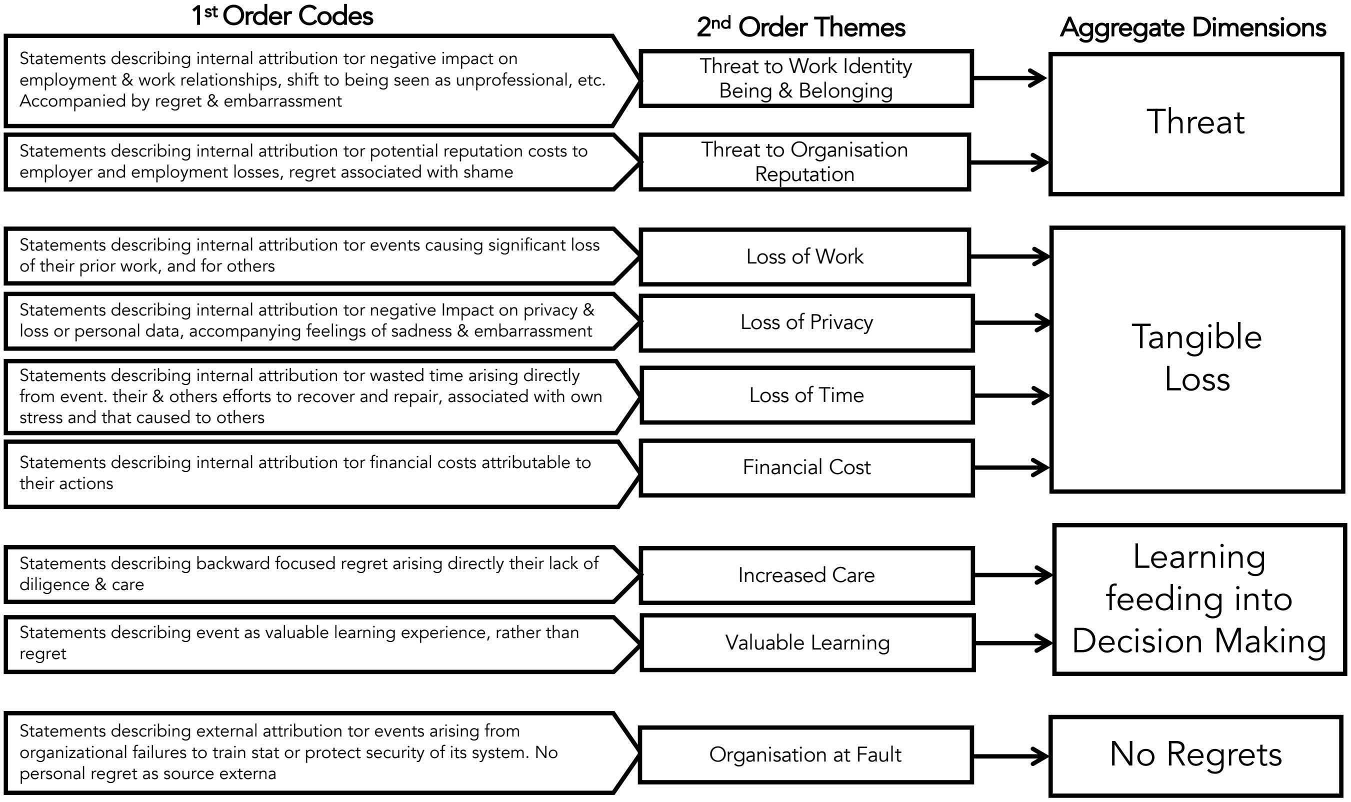
1st Order Codes
2nd Order Themes
Aggregate Dimensions
Statements describing internal attribution tor negative impact on employment & work relationships, shift to being seen as unprofessional, etc. Accompanied by regret & embarrassment
Threat to Work Identity Being & Belonging
Statements describing internal attribution tor potential reputation costs to employer and employment losses, regret associated with shame
Threat to Organisation Reputation
Threat
Statements describing internal attribution tor events causing significant loss of their prior work, and for others
Loss of Work
Statements describing internal attribution tor negative Impact on privacy & loss or personal data, accompanying feelings of sadness & embarrassment
Loss of Privacy
Statements describing internal attribution tor wasted time arising directly from event. their & others efforts to recover and repair, associated with own stress and that caused to others
Loss of Time
Statements describing internal attribution tor financial costs attributable to their actions
Financial Cost
Tangible Loss
Statements describing backward focused regret arising directly their lack of diligence & care
Increased Care
Statements describing event as valuable learning experience, rather than regret
Valuable Learning
Learning feeding into Decision Making
Statements describing external attribution tor events arising from organizational failures to train stat or protect security of its system. No personal regret as source externa
Organisation at Fault
No Regrets

Figure 4: Themes Generated

5 FINDINGS AND THEMES

5.1 RQ1: Cybersecurity Regret Characteristics

Review of the type of cybersecurity events respondents' encountered indicated four main, and largely similar sized forms. The most frequent type of event related to **poor security** (29%) These ranged from the failure to include up-to-date security software, for example: "*My boss was frugal and did not want to pay the small fee to renew our office's computer security software. The computers were left vulnerable and because of this we lost years of patient dental records and digital Xrays*" (R178).

Security was also compromised by poor individual practices, as the following example illustrates, with the sharing of passwords between co-workers. This led to subsequent high risk misuse of work time and equipment to access unsafe websites: "*Someone in my office was locked out of the server on their computer, so they borrowed my password so they could access the server. Everything was fine, but then that person used my password weeks later to access the server to do something against company policy. They were surfing porn site on their work computer after having gained server access via my password*" (R94).

Malware was the second most frequent type of experience (27%), with either direct or indirect experiences of malware: "*One of our office workers was using a computer for personal business. He opened an email and released malware into our network which caused our computers to slow down to the point that they were not usable*" (R69). In this example, the respondent reflects on the significant consequences of this simple mistake.

A related cybersecurity experience involved **phishing attacks** (24%). While respondents might have some uncertainty about the precise form of malware, they were aware of the adverse consequences that arose, as the following quote reveals: "*Well, I am assuming I clicked on a phishing link, although I am not entirely sure. I am only sure of the outcome, as it seems someone got into my information and opened a bank account in my name, took out a credit card, and hacked into my bank account*" (R371).

The final type of event concerned **backing-up** their information (21%). Here, the experiences often referred to human error, with files accidentally deleted, as the next quote indicates: "*When attempting to use a backup I somehow deleted the current backup instead of the old backup. I realized this after being in recovery mode and already panicking. The old backup would be useful but it did not have enough information to make it relevant. There would be a few things that could be utilized. Ultimately I made a careless mistake, regardless of the reason*" (R300). Sometimes poor back-up processes causes issues: "*We were using this database at work and it stop working. The backup was from too long ago that some of the data was not able to be recovered*" (R363). Backup issues could also arise from unexpected events, including electrical power failures, as this quote shows: "*We were trying to access critical data that was important for an project, but all the information one day due to a critical power outage was* *corrupted. Due to the fact that I did not back up the data properly*" (R368).

Examining what participants' regrets revealed four distinct themes, comprising of 10 sub-themes (see Figure 4). These themes will now be outlined in more detail and illustrated using a typical quote drawn from our coded data set. Each is reported using the respondent ID from the total dataset.

5.1.1 ***Threats:*** An important main theme that emerged was related to threats, comprising two distinct sub-themes.

Threat to Work Identity: This most frequent kind of regret focused on the employee and their professional identity and standing and their relationship with others at work (n=58). This confirms the social dimension of regret outlined in Section 3.1. Responses revealed a dominance of internal attributions, positing these events as a consequence of *their* actions, as the next quote reveals: "*Because I should not have been browsing the internet for non-work related things. It was my fault because instead of looking for something productive to do, I instead started browsing online and looking up pages on social media, shopping pages and the like*" (R265). This points to the following dimensions of this particular regret: agentic, deliberate, past, commission and irreversible.

The outcome raised questions about their work identity, as it appeared to be at odds with how they would like to be seen within their work context: "*Because I looked like a moron and a porn hungry employee*" (R210). Inherent in many of these regret responses was the further emotion of embarrassment, derived from how they might appear to others or anticipating others' responses to their actions, as the next quote typifies: "*It was embarrassing. It made me look stupid in front of IT and other people I worked with. I felt like they were laughing at me and judging me*" (296). This social dimension to their regret is a significant concern.

These experiences could be tinged with shame [83], derived from how their actions now appeared to others in their social work network or externally, signalling a lack of diligence, or simple carelessness. These reflections revealed concerns about their being and belonging in the workplace.

Threat to Organisational Reputation: A second associated source of regret was the threat their actions constituted to their employer, raising concerns about reputational loss and potential questions about the suitability of their policies and processes (n=26). The next quote is typical of this employer-focused regret: "*I regret for the files and folders were very important to my company. That files and folders includes many important information about my company and its branches*" (R99).

Respondents were clear about their role in triggering these events, as the following quote demonstrates, with internal attribution related to how their actions escalated the threat to their employer: "*The breach was due to an oversight on my part, and a belief that the functions that I performed on the PC would not be subject to any appreciable risk. This ultimately was proven wrong and placed my companies information at risk. Its a mistake that I won't make again*" (R238).

These two themes outlined different forms of threat resulting from these regret experiences, with some clear inter-relationships in the threats the event posed to the individual and their employer, as the next quote illustrates: "*Because even though nothing really bad happened, it compromised my employer and made me look bad*" (R342).

5.1.2 ***Losses:*** A significant theme related to the consequences that arose from these events, with four sub-themes that identified distinct types of losses that were incurred.

Loss of Work – The most frequent was the cost of these events in terms of lost work, or the effort that was wasted, or required to recover or repair the situation (n=58). The following quote provides a typical example indicating the costs of this waste, but also its spillover consequences especially for IT services. It also hints at an underlying negative emotional component associated with reaction that added to the experience of regret : "*It cost me valuable work time and the consternation of the IT department for infecting my computer*" (R350).

Loss of Privacy – The second most frequent loss was more personal, and also exposure (n=44). In these cases, some of personal value to them had been lost, and involved distinct associated emotions including sadness and vulnerability, rather than embarrassment. The following example highlights not only poor working practices, and organisational software, but also the merging of work with home, so the consequences of cybersecurity breaches extended in poignant ways. For example: "*I was in the middle of a chain of emails between my entire department. We never deleted conversations and our mail service software did a really bad job at organizing the mess, so it was easy for things to fly through unsuspectingly. Within our chain one of the emails had a link and the context of the message was in line with what everyone was talking about so we didn't think anything less of it. Once we clicked on the link it required us to sign in to view the calendar entries. After signing-in the next page that loaded was a white blank page. I remember trying to login numerous times thinking it was some error until I saw the next email that my password had been changed. My email account had many attachments from coworkers, and family/friends. All those files were lost as the company was unable to retrieve everything that was deleted after gaining access back to the account. I'll never get those photos back and all those important memories will slowly fade as time moves on. Pictures like my niece acting like she was working from home when she was in school might be just funny, but it had a lot of sentimental value beyond that*" (R119). The personal costs could also include relationships, with breaches of trust that could have had far more significant personal consequences: "*I trusted the person so much but he broke my trust and what he did nearly cost me my job because i trusted the wrong person*" (R191).

Loss of Time – Related to the cost of work, there was also specific mention of the time wasted directly from these experiences (n=31), often trying to recover what had been lost, as the next quote exemplifies: "*We recently switched to completely new computers at work, a significant upgrade from our old system. Unfortunately, I had saved a number of important files directly to my old computer and forgot to copy or retrieve them before the IT company switched the equipment. Nothing vital was lost, but it was still frustrating and caused me to lose a lot of time chasing files down... Many of the files that were lost had information and reports on previous events, and reconstructing that information cost me a lot of time and effort that could have been used better elsewhere*" (R274). The loss of time often involved anxiety and stress, which was not just confined to the individual, as the next quote indicates: "*The lost time, the hassle, the stress of having to then triple-check everything for accuracy was my main regret. I felt like a careless mistake that could have so easily been avoided took a lot of time and freedom away from me*" (R185). The temporal loss could also spill over into new anxiety and concerns about other work-related parties, for example: "*I regret it because it not only lost me work hours, but it also makes me question all of my coworkers around me now*" (R214). It could also lead to additional wasted time and work for others, as the following quote outlines: "*I regret what happened because it took a lot of time and effort to clear my computer of all the issues the person that got into it from clicking the link, IT had to come work on my computer for quite some time, and I also had to change all my passwords on my computer, and also because of what I did, everyone in my office had to sit through a 2 hour cybersecurity class at work*" (R229).

Loss of Finance – The final sub-theme here concerns financial losses (N=5). The monetary costs from these events was often combined with other losses, notably time or effort, and is illustrated in this typical quote: "*I regret it because I had to spend money and it also took a lot of my time to get the computer fixed*" (R204).

5.1.3 *Learning:*

These cybersecurity events and the regrets they could trigger had two important impacts that concern distinct individual responses, including greater care and valuable learning.

Increased Care: Experiences of regret in some respondents were regarded as a backward-focused phenomena that concerned just the specific event and the issues, such as how their lack of diligence triggered the event. These responses tended to identify a short-term and narrowly focused insight as the next quote illustrates: "*I have the same mentality about the situation now as I did back then, but I was forgetful and in a rush on the day that it happened*" (R92). In these cases, the event could lead to behavioural changes, notably greater caution and care being taken in similar contexts, as this next quote reveals: "*I should have never even been tricked by the phishing email. I am much more careful about clicking on any links in unsolicited emails*" (R257). These respondents noted how their lack of diligence and care contributed, and so were more aware of the need to be careful (N=55).

While some respondents revealed dramatic consequences from the experiences, for others it was far less significant. Yet, it created a huge impact on their subsequent actions, as the next quote demonstrates following a poor virus protection experience: "*In hindsight, this breach pointed out the importance of being adequately protected against potential threats. Even though my work on the PC was relatively low risk, it was still able to be compromised...The breach was due to an oversight on my part, and a belief that the functions that I performed on the PC would not be subject to any appreciable risks. This ultimately was proven wrong and placed my company's information at risk. It's a mistake that I won't make again*" (R238).

These cases revealed the salience of the threat and the risk that could be incurred making it more germane for individuals.

Valuable Learning Opportunity: Interestingly, but less frequently, were respondents who did not regard these experience so negatively. Hence, the event was not regarded as something to regret. Instead, it offered a seminal anchoring event that afforded significant learning opportunities (N=9). Critically, these individuals indicated clear internal attributions for event as they following example shows: "*I lost a file I had been working on for weeks. I learned from my mistake and always back-up my files before closing my program...I regret that it happened because I was careless but it was a learning experience*" (R320). Importantly, they identified a significant change to their current and future behaviours formed from the experience. In this way, they shifted the emphasis from regret to the experience's value for them as this quote captures: "*Yes, but only slightly. In the long run it actually made me better.*"(R311).

The events, however, did not have to be direct experiences as the next example highlights: "*I learned a valuable lesson at someone else's expense. I don't regret it.*" (R112). Although the individual does not discern the feelings of regret, arising from their internal attribution of cause, they see its significance recognising how it could very easily have happened to them.

5.1.4 *No Regrets:*

These respondents (n=15) were aware that something significant and negative had occurred, but the impact on them and their current and future actions was limited, as the next quote reveals: "*I was extremely concerned and tried to understand how something like that could happened. I know I did not do anything different that I would normally do.*" (R253). These experiences were regarded by respondents as incomprehensible, removing feeling of regret. It is thus rendered as without relevance them personally, as the next quote indicates: "*I can't exactly regret it since there was nothing that I did wrong.*" (R154). These types of events were characterised by an external attribution about what had occurred, for example "*I don't regret it because I didn't cause it. i certainly wish it did not happen. We lost 4 days of productivity overall*" (R244). They did note the costs for them, but deflected why it arose, identifying the causal locus as resting with their employing organisation, such as "*Take some action to awareness to the employees and the system users.*" (R73).

Others regarded these events as 'unicorn' experiences that would not occur to them, for example "*I do not have any regrets due to my diligence in security.*" (R192). This may be accurate, or severely deluded, our data collection makes checking its validity impossible.

5.1.5 *What could be Done Differently?*

We invited participants to reflect on what could be done differently in these experiences, with three suggestions identified. Most frequent was the need to take more active precautions (N=88). *First* they reflected on the more effective use of existing systems, such as backing-up files, saving data in more secure places, and actively logging out of personal accounts. An important component here was prior planning, and not making assumptions that took security for granted. A *second* theme concerned individuals' effort and attention (n=59). Here, the emphasis was on being more "cyber-aware" through paying active attention to important details for example an address or link included in an email, and deliberately avoiding unsafe websites. A *final* approach focused on the external organisational resources that either included greater levels of workplace training, or more advanced security systems (n=26). Frequently noted were training and awareness raising by the employing organisation.

5.2 RQ2: *Anticipated Regret*

Direct experiences of regret that arose from malware, poor security and phishing events appeared to have the largest impact on current and future behaviour. They often resulted in actions that were now regretted, as the behaviour had made the threat more salient, as the next quote shows: "*I took home a hard drive that I should not have without properly backing it up and it failed while I was using it....I am now much more careful to have myself covered or protected from these types of incidents*" (R203). These examples involved respondents indicate their own culpability and lack of diligence that lead to significant issues for organisations and themselves and which they regretted (see Figure 3). The prior event helped forge a new awareness of the risks and lead directly to more secure behaviour as the next quote indicates: "*I didn't think anyone would bother to steal my passwords, because I don't deal with large amount of money or credit, but now I know better*" (R121).

The use of experiences to anticipate what could occur could be significant even if they were not directly effected. As example of these anticipated regrets arose in the next quote where the playing of a practical joke had illuminated the salience of the risks from not closing down your system before leaving it unattended: "*This was not me but one of my employees. My assistant left her computer on and email up when she left work. Our boss, a friend of hers, got on her email and sent another employee a fake romantic email, then shut down the computer. The next morning the employee who received the email (who had a good sense of humor) went to our boss to report what happened. The boss let her in on the joke. The employee who received the email played along and replied. When my employee came in she was flummoxed, we all had a laugh, but I learned a VERY valuable lesson!*" (R207).

Significantly, these experiences were not confined to a single point in time, instead the sense-making that followed revealed that individuals returned to these experience to ruminate about what had happened and sense-making about why the outcome was not as anticipated. The next quote captures how initial insights about their culpability could change as they became more aware of what the organisation could have done better: "*For one, I am much more knowledgeable about cybersecurity issues and how to better avoid them now. At the time, it was terribly embarrassing and stressful because I assumed I would get in more trouble than I did. Then, I placed the blame solely on myself. Now, I understand that my employer should have, at the very least, given me some basic training on cybersecurity threats, since my job heavily involved the use of a computer*" (R373). These shifts in perspective are accompanied by initial negative emotions associated with self-consciousness and self-blame, which are now re-framed in the light of subsequent knowledge to understanding their position within a wider system in which the role should have been better supported.

In contrast to these efforts by individuals to understand and apply their new insight to current and future activities, examples were found of organisations who were seen as deliberately playing with, and embarrassing employees. These reflections suggest a squandering of the valuable learning from anticipated regret, as one respondent reflected: "*We also will sometimes be tested with phishing emails designed to trick us....I would find a phishing email in my inbox one morning and then have to click to report it to IT. I already know that they are sending these out as a test to see who is not compliant.*"(R314), or passive responses, including "*They just sent an email with a pdf*" (R120).

5.3 RQ3: *Experienced Regret*

While there were examples of the use of experiences to then anticipate and transfer their new awareness, there were examples of experiences that were more confined, as the following quote captures: "*I regret what happened because it was incredibly stressful at the time and I thought I was going to lose everything on my computer*" (R323). It shows insight into a potentially far more negative outcome. Similarly even those with some more advanced knowledge were found to undertake surprisingly naïve behaviours, as this next example shows, "*I looked up the term "sex swing", unsure of what it was, and clicked on a link. Within a day there were so many pop-ups of pornography pictures that my computer would not function at all. I ended up having to contract a computer repair man to fix the problem. It took him several days to repair the problem, citing it was the worst he had ever seen. It was embarrassing due to the nature of the problem and equally as frustrating given that I have a minor in computer science and was unable to fix the problem myself.*"(R98). This latter examples challenges the earlier assertion (R192) that individual diligence is a insulator.

Regret from these experiences could become segregated arising from concerns about external social threats, such as being reprimanded by line managers, and feelings of embarrassment and fear from co-workers. In these examples, individuals' attention was diverted away from informing cybersecurity behaviours, rather, it led to cynicism about other thwarted organisational outcomes, a future promotions from *that* employer, as the next quote indicates: "*I had lost my important files in my office. The file would be more important for my project work. I was scolded by my team leader. I felt worried about this event....This incident made me embarrassed and worried in front of my coworkers. This event was differently to me...This event had been dangerous to my work. It stopped me to attain next level in my office*" (R105). Instead of learning about how to alter their cybersecurity behaviour, the shame components of these experienced regret events diminished individual's self-scrutiny. As Renaud *et al.* [83] found, shame makes individuals want to move on, rapidly.

The severity of the consequences of cybersecurity events could contribute to this myopia, with efforts being diverted to respond to outcome containment. These events necessitated the involvement of multiple agencies, and made salient negative outcomes that could also have been more sever as the next quote shows: "*It took me months to correct my status. I had to sign up for credit monitoring and make a police report. I also had the fear of unemployment applying a bad record to my file*" (R298). Direct regret experiences could deliver significant changes to cybersecurity behaviours as the following example indicates: "*I am more alert to what information I give out. I do not readily give my social security number unless absolutely required. I also will avoid an address if it is optional*" (R298).

Ongoing rumination was a feature of direct regret experiences. They arose as part of the drive to make sense of opaque events with active sense-making apparent in the next examples starting with respondent 72 who reflected - "*I don't know how it happened but many important files were erased. They completely disappeared and* *were nowhere to be found. It's still a mystery how this happened and it cost us a lot of problems at work. It was a definite set back. These were really important files....*". When asked if they saw the experience differently now, note the key hallmarks of regret with its ongoing negative emotions and unresolved cognitions concerning the event alongside clear learning guiding their future actions designed to reduce its further occurrence: " *I don't see it differently except I now learned what we need to do to make sure this never happens again. I'm still just as upset and mystified as I was when this first happened. It's still very confusing and aggravating.*"

An important divergence from anticipated regret is the salience of these event's legacy in the present and future, retaining the ongoing potential to re-exposure the individual to further threat, as the next quote shows: "*Because I lost personal details and hackers can find different ways to get access to my accounts*" (R98). They are clear in the attribution of who is to blame for this outcome.

6 DISCUSSION & REFLECTION

Our exploratory study of regret within a cybersecurity context shows regret to be a salient emotion.

Process Model Confirmation.
Our findings confirm some of the actions in the process model depicted in Figure 3. It arises when scrutinising an expected (cmp9) and actual outcome (cmp12) that reveals a divergence that aligns with the comparison stage, which is accompanied by negative emotions and ongoing meaning-making (cmp19) that has implications for their own and others' current and future actions. They draw from their experiences (cmp3) and those of others to discern actual outcomes (cmp12) but also recognise its potential consequences (cmp2 or cmp16) in terms of losses in four areas: work (when files have been lost), privacy (where personal files are lost, or their device breached), time (needed to recover), and financial loss. In these reviews, evidence is found that corresponds with three distinct process areas (see Figure 3) including: decision making, action & appraisal and experienced regret. Notably, we find that decision-making includes discerning causal connections (cmp8) aimed at trying to understand why event arose, expressing concerns about the immediate consequences of the occurrence on their employing organisation and/or themselves.

Critically, the consequent actions revolve around the attributions of responsibility, distinguishing between themselves (cmp8), or other parties (cmp5), notably the organisation. However, these consequences may not be stable, instead revealing a dynamic, that denotes rumination (cmp19), especially in the discernment of responsibility that shifts from the individual (cmp14), onto the organisation (cmp15). These ruminations can be accompanied by strong negative emotions. Importantly, while we asked about experiences of regret, analysis of responses denote different outcomes for regret where an individual can externalise blame and lay responsibility onto the organisation. This reduces their learning and potential future behavioural change due to a diminishing of individual attention and effort around cybersecurity (see Figure 5). For example, one respondent's (R178) very frugal, but short-sighted boss would not pay the security subscription, leaving all of the organisation's devices vulnerable. When the inevitable data breach occurred, the respondent regretted all the time the partial recovery of lost data took, but they were clear where blame lay and what changes were needed. These cases indicate the challenge of utilising regret, especially anticipated regret, where there is an external attribution of blame.

In contrast, where regret lay with the individual, we found instances of rejoicing at the severity of what could have happened but did not (cmp22), as well drawing from these events that recognised their implications in the present and more long term (cmp2). This informed subsequent decision-making processes and actions (see Figure 5). Our respondents made an effort to look for the positives of the event (cmp22), and well as a desire for a different present and future (cmp21). Important to cybersecurity, they demonstrate that regret is significant in reshaping understanding of threats and that the salience of these aforementioned losses can underpin changes in behaviour. For example, the respondent who shared a password and almost lost their job as a consequence concluded that they had been too trusting and would no longer share passwords.

Counterfactual Thinking.
Kahneman and Tversky [51] call regret the counterfactual emotion. Regret thus offers us the capacity to engage more comprehensively with experiences and to explicate from experiences to consider what could have and might have arisen [75]. It can be a difficult process as it might involve admitting socially undesirable or embarrassing events and outcomes. However, it is an important means of extracting learning, with a few of our respondents indicating counterfactual thinking. These insights involved recognising that there were near misses, where they had been and hoped to remain lucky as they were now aware that they had not exercised sufficient care. These examples showed instances of self-recrimination and self insight about what nearly was; the suggestion of culpability that is hard to disclose was evident in omissions as well as actions - notable from failures to back-up or be duly attentive.

One important mechanism to prime such thinking arose from reactions to other's experiences and the recognition of their transferal onto their own lives. We found instances of profound vicarious learning, as individuals reflected on another's outcome and how it could have been them. For example, from a practical joke on a computer left attended and signed-on. The adverse experiences of others might be more palatable means of engaging recognition of threats and salient vulnerabilities, without the associated embarrassment or potential shaming [81].

By contrast, as the earlier section denotes, despite asking respondents to reflect on a regret, it was far easier and more comfortable for individuals to deflect attention onto the culpability of others, or to view themselves are impervious to such events. Our examples however offer important challenge to this omission of counterfactual thinking, including wishing the event had not happened and insight into the speed at which everything unravelled, that left limited time for clear thinking. Reviewing these examples and capturing their own near misses might be a useful resources to consider an event's fallout, focus on making sense about whether it could occur in *their* context.

Lessons Learned.
Extant study contends regret to be a beneficial emotion, in that it allows people to scrutinise and learn from their mistakes (e.g.

[75]. Regret-informed learning was evident for individuals and their colleagues from even fairly minor incidents that made salient how a major incident could have arisen. These raised awareness about actual threat levels. They reveal how valuable these lessons could be for organisational cybersecurity, highlighting the possibility of being exposed and introducing an opportunity to try and apply their knowledge. These experiences make salient the concerns for an organisation and its employees, for example: "*When it actually happens to you, that really changes everything. You loose your sense of security (no pun intended) but you learn a life lesson through Hard Knocks. That's the best school. I reacted quickly and did the right thing. I did not panic and acted right away. It made me focus and think very quickly. I learned a lot and my team learned a lot. I guess we all learned a lot and even more since there were a total of about 40+ emails with that malware that day. It is better to learn with a minor incident than with a big incident. That is the main reason I don't regret it. We were able to get some "Good" out of it and "rehearsed" our Cyber Alerts, etc...*". As a result, respondents themselves were very aware of what they had learnt from the experience and the changes produced in their current and future actions, such as greater care or scrutiny.

Important factors in regret learning arose where causality was unclear with the root cause being difficult to pinpoint. This opacity could arise where they did not regard themselves as being to blame for the occurrence, or failing to acknowledge how they could have done things differently. In cases where the person does not understand why and how the event came to occur, and they have no feelings of regret, the link to future actions may be lost. We observed many examples including those described by R244, where no one knew how the malware had entered their organisation. No regret resulted and so no learning could take place which could inform future decision making.

A second factor reducing learning occurred where blame was deflected onto others or the organisation, losing even anticipated learning opportunities. Here, the resultant ongoing sense-making could shift dynamically from regret and self-blame towards viewing the employing organisation as derelict in its duty. This outcome was denoted by failures to provide necessary awareness-raising and training, leaving employees who work with sensitive information vulnerable. In these cases, respondents indicated that despite responding to a question about regret they did not attend to and learn from their experience as they were not responsible.

A further feature of the type of lessons learned aligns with prior studies about differences between private experiences, as compared to those open to social scrutiny (e.g.[107]). In events where others were aware, individuals were concerned about the impact on their social standing with peers, or superiors, and the consequences for their employer and ongoing employment. They show concerns about work identity and their perceived capability [112]. Depending on how the organisation manages the fallout, feelings of shame and alienation could occur [83]. This social dimension as well as the associated negative feelings could diminish self-scrutiny and -reflection.

6.1 Research Implications

This exploratory study shows regret as an important element in experiences of cybersecurity breach. These results support a process model concerning regret and its distinct forms. However, we are implying and not testing causality. The model reveals the kinds of issues that manifest, and the important factors for regret. Further research is valuable to test out these suggested relationships. An important aspect to explore further concerns private events as compared to social. Future study could also consider the merit of near miss review, to extend opportunities for counterfactual thinking that our study design was ill adapted for. Methods including in-depth interview and longitudinal experiment would be of particular value here.

Prior research into cybersecurity and the use of fear appeals by Renaud & Dupuis [81] led us to question whether fear was really being triggered. Dupuis *et al.* [23] found that although fear *was* indeed triggered, so were other negative emotions. We take this challenge a step further to question: are fear appeals perhaps eliciting a sense of anticipated regret, or even dread, rather than fear?

Fear is defined as "*an unpleasant emotion caused by the threat of danger, pain, or harm*", while dread is defined as "*anticipate with great apprehension or fear*". It seems then that dread is almost a "fear of fear". Is this what fear appeals are really triggering? Moreover, would an anticipated cyber event really cause fear of an existential threat, which is implied by this definition, or rather dread of the embarrassment and shame if one were to trigger a cyber incident?

However, instead of a fear-based emotion, let us consider the possibility that regret might be the relevant emotion in these kinds of appeals, defined as "*feel sad, repentant, or disappointed over*". In the same way that dread is linked to fear, does a regret appeal trigger an anticipation of sadness or disappointment denoting regret is experienced? This would suggest hat fear appeal is not the right label. The distinctions between these different, yet related, terms are not merely academic; It is important to understand the negative emotions that are being triggered, to allow more informed choices about interventions in handling adverse cybersecurity incidents. This is a fruitful avenue for future research.

6.2 Practical Implications

The point of regret appeals is to make people think about and engage with the future consequences of their actions. There are other ways to achieve this that do not involve invoking negative emotions. For example, McGonigal [68] argues that serious educational games enable access to possible futures, helping to forecast outcomes and inform decision.

The likelihood of regret becoming a positive outcome depends on the attribution. Our research participants show internal attribution as more likely where the organisation has a cybersecurity education, training, and awareness program user recall and have engaged in, even if not fully effective 100% of the time. In these cases, regret could shift into learning in the long-term if a mistake can be reviewed and counterfactual thinking primed.

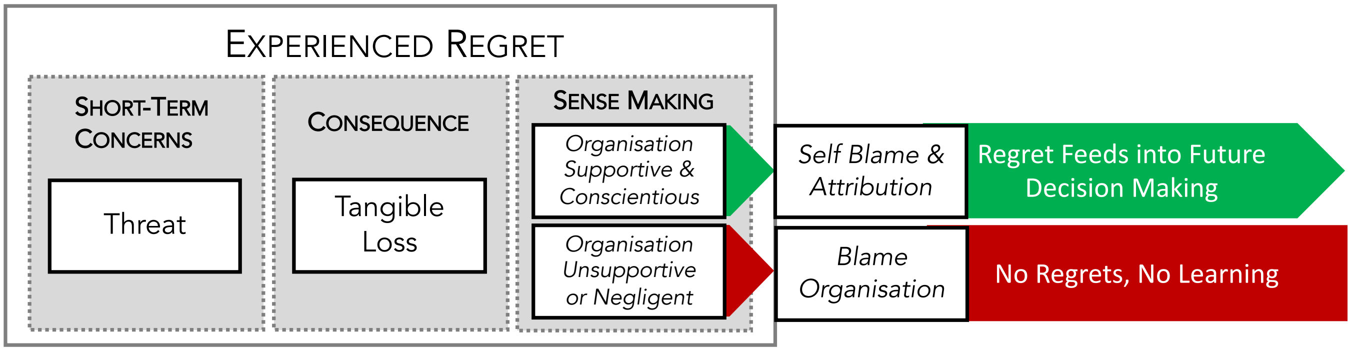

Figure 5: Theme Summary & Implications

6.3 Limitations

There are several limitations worth noting. *First*, this was a single survey using a crowd-sourced participant pool. While compensation was considered fair by most, MTurk workers do have an incentive to complete the work as quickly as possible. Thus, some responses and their overall attention may not be optimal. We believe our additional quality control checks helped mitigate this issue, but it cannot be fully eliminated. Supplementary analysis using interviews were allow further probing and clarification of what was meant.

Second, data was collected for this study via a survey, thus, common method bias is a concern [78]. We did implement several quality control procedures to address and reduce this concern. Furthermore, the anonymity of participants completing the survey may offer freedom to diligence embarrassing experiences. Therefore, while certain components of the procedures used and the participant pool employed help to minimise the chance that common method bias was a significant issue in the results we obtained, it nonetheless remains a concern.

Third, the data we collected comes from a single snapshot in time for our participants. This has not the means to show causality that a longitudinal study would afford. We do not know whether the actions reported as regret were influenced by other extraneous factors occurring while they completed the survey.

Finally, we do not know whether any emotional harm resulted from the recollection of events that they may have regretted — some of which were significant. While this study was considered low risk and approved as exempt from a full IRB review, it is possible that recalling such events may be emotionally troubling for some individuals.

7 CONCLUSION & FUTURE WORK

We sought to understand the role of regret in cybersecurity. The research literature suggested a process model of regret but we did not know whether this would also accurately reflect cybersecurity regrets. We received 427 valid responses from crowd workers regarding a cybersecurity experience they had at work that they regretted and discovered that people did indeed go through various stages after an adverse event, but we did not find evidence for counterfactual thinking. We have delineated the characteristics of regret to differentiate the two forms and the importance of learning that regret can lead to. Future work that picks apart the differences between regret, fear and dread would be valuable, to understand how best to manage and satisfy employees' cybersecurity expectations in organisations. Specifically, if organisations are going to use interventions that trigger these emotions, it is necessary to understand exactly how they work. Finally, it would be beneficial to interview those who have experienced regret in the cyber domain, to probe their experiences and emotions, as well as the learning potential of regrettable events.

REFERENCES

[1] Basel Abdelazeem, Kirellos Said Abbas, Mostafa Atef Amin, Nahla Ahmed El-Shahat, Bilal Malik, Atefeh Kalantary, and Mostafa Eltobgy. 2022. The effectiveness of incentives for research participation: A systematic review and meta-analysis of randomized controlled trials. *PLOS ONE* 17, 4 (Apr 2022), e0267534. https://doi.org/10.1371/journal.pone.0267534

[2] Charles Abraham and Paschal Sheeran. 2003. Acting on intentions: The role of anticipated regret. *British Journal of Social Psychology* 42, 4 (2003), 495–511.

[3] Dolores Albarracín, Aashna Sunderrajan, Wenhao Dai, and Benjamin X White. 2019. The social creation of action and inaction: From concepts to goals to behaviors. In *Advances in Experimental Social Psychology*, James M Olsen (Ed.). Vol. 60. Elsevier, Cambridge, USA, 223–271.

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

[5] Denise R. Beike, Keith D. Markman, and Figen Karadogan. 2009. What we regret most are lost opportunities: A theory of regret intensity. *Personality and Social Psychology Bulletin* 35, 3 (2009), 385–397.

[6] David E Bell. 1985. Reply—Putting a premium on regret. *Management Science* 31, 1 (1985), 117–122.

[7] Leonard Berkowitz. 1990. On the formation and regulation of anger and aggression: A cognitive-neoassociationistic analysis. *American Psychologist* 45, 4 (1990), 494.

[8] Mariëtte Berndsen, Joop van der Pligt, Bertjan Doosje, and Antony Manstead. 2004. Guilt and regret: The determining role of interpersonal and intrapersonal harm. *Cognition and Emotion* 18, 1 (2004), 55–70.

[9] Pär Bjälkebring, Daniel Västfjäll, Ola Svenson, and Paul Slovic. 2016. Regulation of experienced and anticipated regret in daily decision making. *Emotion* 16, 3 (2016), 381–386.

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

[11] Seger M Breugelmans, Marcel Zeelenberg, Thomas Gilovich, Wen-Hsien Huang, and Yaniv Shani. 2014. Generality and cultural variation in the experience of regret. *Emotion* 14, 6 (2014), 1037–1048.

[12] Noel T. Brewer, Jessica T. DeFrank, and Melissa B. Gilkey. 2016. Anticipated regret and health behavior: A meta-analysis. *Health Psychology* 35, 11 (2016), 1264–1275.

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

[14] Terry Connolly and Jochen Reb. 2005. Regret in Cancer-Related Decisions. *Health Psychology* 24, 4S (2005), S29–S34.

[15] Terry Connolly and Marcel Zeelenberg. 2002. Regret in decision making. *Current Directions in Psychological Science* 11, 6 (2002), 212–216.

[16] Giorgio Coricelli, Raymond J Dolan, and Angela Sirigu. 2007. Brain, emotion and decision making: the paradigmatic example of regret. *Trends in Cognitive Sciences* 11, 6 (2007), 258–265.

[17] Joel Crawford, Andrew Jones, Abi Rose, and Richard Cooke. 2022. 'You see the pictures the morning after and you're like I wish I was in them': an interpretative phenomenological analysis of university student's alcohol-related regrets. *Psychology & Health* 37, 4 (2022), 490–506.

[18] Matthew T Crawford, Allen R McConnell, Amy C Lewis, and Steven J Sherman. 2002. Reactance, compliance, and anticipated regret. *Journal of Experimental Social Psychology* 38, 1 (2002), 56–63.

[19] Michael Davern, Todd H. Rockwood, Randy Sherrod, and Stephen Campbell. 2003. Prepaid monetary incentives and data quality in face-to-face interviews: Data from the 1996 survey of income and program participation incentive experiment. *The Public Opinion Quarterly* 67, 1 (2003), 139–147.

[20] Marlies de Groot, Juliette Schaafsma, Thomas Castelain, Katarzyna Malinowska, Liesbeth Mann, Yohsuke Ohtsubo, Maria Theresia Asti Wulandari, Ruba Fahmi Bataineh, Douglas P Fry, Martijn Goudbeek, et al. 2021. Group-based shame, guilt, and regret across cultures. *European Journal of Social Psychology* 51, 7 (2021), 1198–1212.

[21] Marc Dupuis, Barbara Endicott-Popovsky, and Robert Crossler. 2013. An Analysis of the Use of Amazon's Mechanical Turk for Survey Research in the Cloud. In *International Conference on Cloud Security Management*, B. Endicott-Popovsky (Ed.). Academic Conferences, Seattle, Washington, 10–17.

[22] Marc Dupuis and Samreen Khadeer. 2016. Curiosity killed the organization: A psychological comparison between malicious and non-malicious insiders and the insider threat. In *Proceedings of the 5th Annual Conference on Research in Information Technology*. ACM, Boston, USA, 35–40.

[23] Marc Dupuis, Karen Renaud, and Anna Jennings. 2022. Fear might motivate secure password choices in the short term, but at what cost?. In *Hawaii International Conference on System Sciences*. IEEE, Online, 1–10.

[24] Maria Madalena d'Avelar. 2022. On Regret: A Sociological Intersectional Approach. *Social Sciences* 11, 2 (2022), Paper 50.

[25] Daniel A Effron, Christopher J Bryan, and J Keith Murnighan. 2015. Cheating at the end to avoid regret. *Journal of Personality and Social Psychology* 109, 3 (2015), 395–414.

[26] Kai Epstude and Neal J Roese. 2008. The functional theory of counterfactual thinking. *Personality and Social Psychology Review* 12, 2 (2008), 168–192.

[27] Leon Festinger. 1957. *A theory of cognitive dissonance*. Vol. 2. Stanford University Press, Stanford, California.

[28] Donna L Floyd, Steven Prentice-Dunn, and Ronald W Rogers. 2000. A meta-analysis of research on protection motivation theory. *Journal of Applied Social Psychology* 30, 2 (2000), 407–429.

[29] Daniel T. Gilbert, Carey K. Morewedge, Jane L. Risen, and Timothy D. Wilson. 2004. Looking forward to looking backward: The misprediction of regret. *Psychological Science* 15, 5 (2004), 346–350.

[30] Thomas Gilovich and Victoria Husted Medvec. 1994. The temporal pattern to the experience of regret. *Journal of Personality and Social Psychology* 67, 3 (1994), 357–365.

[31] Thomas Gilovich and Victoria Husted Medvec. 1995. The experience of regret: what, when, and why. *Psychological Review* 102, 2 (1995), 379–395.

[32] Thomas Gilovich, Victoria Husted Medvec, and Daniel Kahneman. 1998. Varieties of regret: A debate and partial resolution. *Psychological Review* 105, 3 (1998), 602–605.

[33] Roger Giner-Sorolla. 2012. Science or art? How aesthetic standards grease the way through the publication bottleneck but undermine science. *Perspectives on Psychological Science* 7, 6 (2012), 562–571.

[34] Gaston Godin and Gerjo Kok. 1996. The theory of planned behavior: a review of its applications to health-related behaviors. *American Journal of Health Promotion* 11, 2 (1996), 87–98.

[35] Stephanie Gootman. 2016. OPM hack: The most dangerous threat to the federal government today. *Journal of Applied Security Research* 11, 4 (2016), 517–525.

[36] Kirsten Grasshof, Barbara Kahn, and Mary Frances Luce. 2007. Fact, Fear, Or Regret: Getting People to Cope Actively. *ACR North American Advances* 34 (2007), 532–535.

[37] Jamie Grierson. 2021. What the loss of records from the Police National Computer means. Retrieved 17 April 2022 from: https://www.theguardian.com/uk-news/2021/jan/15/what-the-loss-of-records-from-the-police-national-computer-means.

[38] Susan W. Groth. 2010. Honorarium or coercion: use of incentives for participants in clinical research. *The Journal of the New York State Nurses' Association* 41, 1 (2010), 11.

[39] Lee Hadlington. 2021. The "human factor" in cybersecurity: Exploring the accidental insider. In *Research Anthology on Artificial Intelligence Applications in Security*. IGI Global, USA, 1960–1977.

[40] Stuart Hampshire. 1983. *Morality and conflict*. Wiley–Blackwell, UK.

[41] Einav Hart, Yaakov Kareev, and Judith Avrahami. 2016. Good times, bad times: Reversal of risk preferences. *Decision* 3, 2 (2016), 132–145.

[42] William M Hayes and Douglas H Wedell. 2021. Regret in experience-based decisions: The effects of expected value differences and mixed gains and losses. *Decision* 8, 4 (2021), 277–294.

[43] Wu He and Zuopeng Zhang. 2019. Enterprise cybersecurity training and awareness programs: Recommendations for success. *Journal of Organizational Computing and Electronic Commerce* 29, 4 (2019), 249–257.

[44] Steven J Heine and Darrin R Lehman. 1999. Culture, self-discrepancies, and self-satisfaction. *Personality and Social Psychology Bulletin* 25, 8 (1999), 915–925.

[45] John J Hetts, David S Boninger, David A Armor, Faith Gleicher, and Ariel Nathanson. 2000. The influence of anticipated counterfactual regret on behavior. *Psychology & Marketing* 17, 4 (2000), 345–368.

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

[47] Bruce A Huhmann and Timothy P Brotherton. 1997. A content analysis of guilt appeals in popular magazine advertisements. *Journal of Advertising* 26, 2 (1997), 35–45.

[48] Ben Irons and Cameron Hepburn. 2007. Regret theory and the tyranny of choice. *Economic Record* 83, 261 (2007), 191–203.

[49] Irving L Janis and Leon Mann. 1977. *Decision making: A psychological analysis of conflict, choice, and commitment*. Free Press, UK.

[50] Daniel Kahneman, Stewart Paul Slovic, Paul Slovic, and Amos Tversky. 1982. *Judgment under uncertainty: Heuristics and biases*. Cambridge University Press, Cambridge, UK.

[51] Daniel Kahneman and Amos Tversky. 1982. The simulation heuristic. In *Judgement under uncertainty: Heuristics and biases*, D Kahneman, P Slovic, and A Tversky (Eds.). Cambridge University Press, Cambridge, UK.

[52] Mitchell Kajzer, John D'Arcy, Charles R Crowell, Aaron Striegel, and Dirk Van Bruggen. 2014. An exploratory investigation of message-person congruence in information security awareness campaigns. *Computers & Security* 43 (2014), 64–76.

[53] Annaysa Salvador Muniz Kamiya, Marcel Zeelenberg, and José Mauro da Costa Hernandez. 2021. Regulating regret via decreasing goal level: Comparing maximizers and satisficers. *Personality and Individual Differences* 178 (2021), 110870.

[54] Toni Kaplan, Susumu Saito, Kotaro Hara, and Jeffrey P. Bigham. 2018. Striving to earn more: a survey of work strategies and tool use among crowd workers. In *Sixth AAAI Conference on Human Computation and Crowdsourcing*. AAAI Press, Zürich, Switzerland, 70–78.

[55] Annalise Kempen. 2016. Cybersecurity-are we making progress in the fight against cybercrime? *Servamus Community-based Safety and Security Magazine* 109, 11 (2016), 19–23.

[56] Ryan Kennedy, Scott Clifford, Tyler Burleigh, Philip D. Waggoner, Ryan Jewell, and Nicholas JG Winter. 2020. The shape of and solutions to the MTurk quality crisis. *Political Science Research and Methods* 8, 4 (2020), 614–629.

[57] Otto F Kernberg. 1985. *Borderline conditions and pathological narcissism*. Rowman & Littlefield, Maryland, USA.

[58] ES Kox, JH Kerstholt, TF Hueting, and PW De Vries. 2021. Trust repair in human-agent teams: the effectiveness of explanations and expressing regret. *Autonomous Agents and Multi-Agent Systems* 35, 2 (2021), 1–20.

[59] Janet Landman. 1987. Regret: A theoretical and conceptual analysis. *Journal for the Theory of Social Behaviour* 17, 2 (1987), 135–160.

[60] Michael Lewis. 1995. Self-conscious emotions. *American Scientist* 83, 1 (1995), 68–78.

[61] Huiyan Lin, Jiafeng Liang, Junkai Yang, and Fei Wu. 2021. Effects of experienced regret on risky decision making are dependent on risky degree. *Scandinavian Journal of Psychology* 62, 3 (2021), 339–347.

[62] Charlie Maclean-Bristol. 2020. Case study - Dundee & Angus College's Cyber Attack communications review. Retrieved 17 April 2022 from: https://planbconsulting.co.uk/knowledge-zone-articles/case-study-dundee-and-angus-colleges-cyber-attack-communications-review/.

[63] Angela T Maitner and Amy Summerville. 2022. "What was meant to be" versus "what might have been": Effects of culture and control on counterfactual thinking. *Journal of Personality and Social Psychology* 123, 1 (2022), 1–27. http://dx.doi.org/10.1037/pspa0000295.

[64] David Mandel. 2003. Counterfactuals, emotions, and context. *Cognition and Emotion* 17, 1 (2003), 139–159.

[65] Luis F Martinez, Marcel Zeelenberg, and John B Rijsman. 2011. Regret, disappointment and the endowment effect. *Journal of Economic Psychology* 32, 6 (2011), 962–968.

[66] Lourdes S Martinez. 2014. Explaining the effects of anticipated regret messages on young women's intention to consume folic acid: a moderated-mediation model. *Journal of Health Communication* 19, 1 (2014), 115–132.

[67] Olimpia Matarazzo, Lucia Abbamonte, Claudia Greco, Barbara Pizzini, and Giovanna Nigro. 2021. Regret and Other Emotions Related to Decision-Making: Antecedents, Appraisals, and Phenomenological Aspects. *Frontiers in Psychology* 12 (2021), 5511. https://www.frontiersin.org/article/10.3389/fpsyg.2021.783248.

[68] Jane McGonigal. 2012. *Reality is broken: Why games make us better and how they can change the world*. Jonathan Cape, London.

[69] Gregory D Moody, Mikko Siponen, and Seppo Pahnila. 2018. Toward a unified model of information security policy compliance. *MIS Quarterly* 42, 1 (2018), 285–A22.

[70] Jonathan Mummolo and Erik Peterson. 2019. Demand effects in survey experiments: An empirical assessment. *American Political Science Review* 113, 2 (2019), 517–529.

[71] Obi Ogbanufe and Robert Pavur. 2022. Going through the emotions of regret and fear: Revisiting protection motivation for identity theft protection. *International Journal of Information Management* 62 (2022), 102432.

[72] Kirsten Passyn. 2019. Adding regret to fear appeals: when the going gets difficult, regret gets action. *Journal of Consumer Affairs* 53, 4 (2019), 1507–1534.

[73] Kirsten Passyn and Mita Sujan. 2006. Self-accountability emotions and fear appeals: Motivating behavior. *Journal of Consumer Research* 32, 4 (2006), 583–589.

[74] Marcello Pericoli and Massimo Sbracia. 2009. The CAPM and the risk appetite index: theoretical differences, empirical similarities, and implementation problems. In *Empirical Similarities, and Implementation Problems*. http://dx.doi.org/10.2139/ssrn.1387462.

[75] Daniel Pink. 2022. *The Power of Regret: How Looking Backward Moves Us Forward.* Canongate Books, Edinburgh, UK.

[76] Daniel Pink. 2022. What Can We Learn from the Solace of 'At Least' and the Sting of 'If Only'? Retrieved 9 March 2022 from: https://behavioralscientist.org/regret-the-solace-of-at-least-and-the-sting-of-if/.

[77] Carolina Pletti, Lorella Lotto, Alessandra Tasso, and Michela Sarlo. 2016. Will I regret it? Anticipated negative emotions modulate choices in moral dilemmas. *Frontiers in Psychology* 7 (2016), 1918.

[78] Philip M. Podsakoff, Scott B. MacKenzie, Jeong-Yeon Lee, and Nathan P. Podsakoff. 2003. Common method biases in behavioral research: a critical review of the literature and recommended remedies. *Journal of Applied Psychology* 88, 5 (2003), 879–903.

[79] Brian Price. 2017. *A theory of regret.* Duke University Press, Durham, UK.

[80] Jochen Reb. 2008. Regret aversion and decision process quality: Effects of regret salience on decision process carefulness. *Organizational Behavior and Human Decision Processes* 105, 2 (2008), 169–182.

[81] Karen Renaud and Marc Dupuis. 2019. Cyber security fear appeals: Unexpectedly complicated. In *Proceedings of the New Security Paradigms Workshop.* IEEE, Costa Rica, 42–56.

[82] Karen Renaud, Robert Otondo, and Merrill Warkentin. 2019. "This is the way 'I' create my passwords"... does the endowment effect deter people from changing the way they create their passwords? *Computers & Security* 82 (2019), 241–260.

[83] Karen Renaud, Rosalind Searle, and Marc Dupuis. 2021. Shame in cyber security: effective behavior modification tool or counterproductive foil?. In *New Security Paradigms Workshop.* IEEE, Online, 70–87.

[84] Karen Renaud and Merrill Warkentin. 2017. Risk homeostasis in information security: challenges in confirming existence and verifying impact. In *Proceedings of the 2017 New Security Paradigms Workshop.* ACM, Santa Cruz, USA, 57–69.

[85] David Resnik. 2015. Bioethical issues in providing financial incentives to research participants. *Medicolegal and Bioethics* (Jun 2015), 35. https://doi.org/10.2147/MB.S70416

[86] Neal J Roese. 1994. The functional basis of counterfactual thinking. *Journal of Personality and Social Psychology* 66, 5 (1994), 805.

[87] Neal J Roese, KAI Epstude, Florian Fessel, Mike Morrison, Rachel Smallman, Amy Summerville, Adam D Galinsky, and Suzanne Segerstrom. 2009. Repetitive regret, depression, and anxiety: Findings from a nationally representative survey. *Journal of Social and Clinical Psychology* 28, 6 (2009), 671–688.

[88] Neal J Roese and Mike Morrison. 2009. The psychology of counterfactual thinking. *Historical Social Research/Historische Sozialforschung* 34, 2 (2009), 16–26.

[89] Neal J. Roese and Amy Summerville. 2005. What we regret most... and why. *Personality and Social Psychology Bulletin* 31, 9 (2005), 1273–1285.

[90] Neal J. Roese, Amy Summerville, and Florian Fessel. 2007. Regret and behavior: Comment on Zeelenberg and Pieters. *Journal of Consumer Psychology* 17, 1 (2007), 25–28.

[91] James A Russell and Albert Mehrabian. 1977. Evidence for a three-factor theory of emotions. *Journal of Research in Personality* 11, 3 (1977), 273–294.

[92] Colleen Saffrey, Amy Summerville, and Neal J. Roese. 2008. Praise for regret: People value regret above other negative emotions. *Motivation and Emotion* 32, 1 (2008), 46–54.

[93] Tracy Sandberg and Mark Conner. 2008. Anticipated regret as an additional predictor in the theory of planned behaviour: A meta-analysis. *British Journal of Social Psychology* 47, 4 (2008), 589–606.

[94] Tracy Sandberg, Russell Hutter, Juliette Richetin, and Mark Conner. 2016. Testing the role of action and inaction anticipated regret on intentions and behaviour. *British Journal of Social Psychology* 55, 3 (2016), 407–425.

[95] David O. Sears. 1986. 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 (1986), 515–530.

[96] Nick Sevdalis, Nigel Harvey, and Michelle Yip. 2006. Regret triggers inaction inertia–but which regret and how? *British Journal of Social Psychology* 45, 4 (2006), 839–853.

[97] Xiaokui Shu, Ke Tian, Andrew Ciambrone, and Danfeng Yao. 2017. Breaking the target: An analysis of target data breach and lessons learned. https://arxiv.org/abs/1701.04940.

[98] Jelle J Sijtsema, Marcel Zeelenberg, and Siegwart M Lindenberg. 2022. Regret, self-regulatory abilities, and well-being: Their intricate relationships. *Journal of Happiness Studies* 23, 3 (2022), 1189–1214.

[99] Itamar Simonson. 1992. The influence of anticipating regret and responsibility on purchase decisions. *Journal of Consumer Research* 19, 1 (1992), 105–118.

[100] Eleanor Singer and Cong Ye. 2013. The use and effects of incentives in surveys. *The ANNALS of the American Academy of Political and Social Science* 645, 1 (2013), 112–141.

[101] Chris MR Smerecnik and Robert AC Ruiter. 2010. Fear appeals in HIV prevention: The role of anticipated regret. *Psychology, Health & Medicine* 15, 5 (2010), 550–559.

[102] Adam Smith. 1822. *The theory of moral sentiments.* Vol. 1. J. Richardson & Co, London.

[103] Richard H Smith, J Matthew Webster, W Gerrod Parrott, and Heidi L Eyre. 2002. The role of public exposure in moral and nonmoral shame and guilt. *Journal of Personality and Social Psychology* 83, 1 (2002), 138–159.

[104] Teodor Sommestad, Henrik Karlzén, and Jonas Hallberg. 2015. The sufficiency of the theory of planned behavior for explaining information security policy compliance. *Information & Computer Security* 23, 2 (2015), 200–217.

[105] Zachary R. Steelman, Bryan I. Hammer, and Moez Limayem. 2014. Data Collection in the Digital Age: Innovative Alternatives to Student Samples. *MIS Quarterly* 38, 2 (2014), 355–378.

[106] Robert Sugden. 1985. Regret, recrimination and rationality. *Theory and Decision* 19, 1 (1985), 77–99.

[107] Amy Summerville and Joshua Buchanan. 2014. Functions of personal experience and of expression of regret. *Personality and Social Psychology Bulletin* 40, 4 (2014), 463–475.

[108] The Gazette. 2018. 'One-man cyber crime wave' who hacked top firms and sold data on dark web jailed. https://www.blackpoolgazette.co.uk/news/crime/one-man-cyber-crime-wave-who-hacked-top-firms-and-sold-data-dark-web-jailed-670523.

[109] Hsin-yi Sandy Tsai, Mengtian Jiang, Saleem Alhabash, Robert LaRose, Nora J Rifon, and Shelia R Cotten. 2016. Understanding online safety behaviors: A protection motivation theory perspective. *Computers & Security* 59 (2016), 138–150.

[110] Michael Tsiros and Vikas Mittal. 2000. Regret: A model of its antecedents and consequences in consumer decision making. *Journal of Consumer Research* 26, 4 (2000), 401–417.

[111] Monique Mitchell Turner and Jill Cornelius Underhill. 2012. Motivating emergency preparedness behaviors: The differential effects of guilt appeals and actually anticipating guilty feelings. *Communication Quarterly* 60, 4 (2012), 545–559.

[112] Job van der Schalk, Toon Kuppens, Martin Bruder, and Antony S.R. Manstead. 2015. The social power of regret: the effect of social appraisal and anticipated emotions on fair and unfair allocations in resource dilemmas. *Journal of Experimental Psychology: General* 144, 1 (2015), 151–157.

[113] Wilco W Van Dijk and Marcel Zeelenberg. 2002. Investigating the appraisal patterns of regret and disappointment. *Motivation and Emotion* 26, 4 (2002), 321–331.

[114] Gerben A Van Kleef, Astrid C Homan, and Arik Cheshin. 2012. Emotional influence at work: Take it EASI. *Organizational Psychology Review* 2, 4 (2012), 311–339.

[115] Tommy Van Steen, Emma Norris, Kirsty Atha, and Adam Joinson. 2020. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? *Journal of Cybersecurity* 6, 1 (2020), tyaa019.

[116] Isabella M. Venter, Rénette J. Blignaut, Karen Renaud, and M. Anja Venter. 2019. Cyber security education is as essential as "The three R's". *Heliyon* 5, 12 (2019), e02855.

[117] Silas Formunyuy Verkijika. 2018. Understanding smartphone security behaviors: An extension of the protection motivation theory with anticipated regret. *Computers & Security* 77 (2018), 860–870.

[118] Silas Formunyuy Verkijika. 2019. "If you know what to do, will you take action to avoid mobile phishing attacks": Self-efficacy, anticipated regret, and gender. *Computers in Human Behavior* 101 (2019), 286–296.

[119] R Jay Wallace. 2013. *The view from here: on affirmation, attachment, and the limits of regret.* Oxford University Press, Oxford.

[120] Merrill Warkentin, Sanjay Goel, Kevin J Williams, and Karen Renaud. 2018. Are we predisposed to behave securely? Influence of risk disposition on individual security behaviors. In *26th European Conference on Information Systems, ECIS 2018.* Association for Information Systems, Portsmouth, UK, 25.

[121] B. Weiner. 1986. Attribution, emotion, and action. In *Handbook of motivation and cognition*, R M Sorrentino and E T Higgin (Eds.). Guilford Press, Guildford, UK, 281—-312.

[122] Alex C. Williams, Gloria Mark, Kristy Milland, Edward Lank, and Edith Law. 2019. The perpetual work life of crowdworkers: How tooling practices increase fragmentation in crowdwork. *Proceedings of the ACM on Human-Computer Interaction* 3, CSCW (2019), 1–28.

[123] Bernard Williams. 1981. *Moral luck: philosophical papers 1973-1980*. Cambridge University Press, Cambridge, UK.

[124] Pamela Wisniewski, Muhammad Irtaza Safi, Sameer Patil, and Xinru Page. 2020. Predicting smartphone location-sharing decisions through self-reflection on past privacy behavior. *Journal of Cybersecurity* 6, 1 (2020), tyaa014.

[125] Kin Fai Ellick Wong and Jessica YY Kwong. 2007. The role of anticipated regret in escalation of commitment. *Journal of Applied Psychology* 92, 2 (2007), 545–554.

[126] Chris Wright and Peter Ayton. 2005. Focusing on what might happen and how it could feel: can the anticipation of regret change students' computing-related choices? *International Journal of Human-Computer Studies* 62, 6 (2005), 759–783.

[127] Antronette K. Yancey, Alexander N. Ortega, and Shiriki K. Kumanyika. 2006. Effective recruitment and retention of minority research participants. *Annu. Rev. Public Health* 27 (2006), 1–28.

[128] Marcel Zeelenberg. 1999. The use of crying over spilled milk: A note on the rationality and functionality of regret. *Philosophical Psychology* 12, 3 (1999), 325–340.

[129] Marcel Zeelenberg and Seger M Breugelmans. 2008. The role of interpersonal harm in distinguishing regret from guilt. *Emotion* 8, 5 (2008), 589–596.

[130] Marcel Zeelenberg and Rik Pieters. 1999. Comparing service delivery to what might have been: Behavioral responses to regret and disappointment. *Journal of Service Research* 2, 1 (1999), 86–97.

[131] Marcel Zeelenberg and Rik Pieters. 2004. Consequences of regret aversion in real life: The case of the Dutch postcode lottery. *Organizational Behavior and Human Decision Processes* 93, 2 (2004), 155–168.

[132] Marcel Zeelenberg, Kees Van den Bos, Eric Van Dijk, and Rik Pieters. 2002. The inaction effect in the psychology of regret. *Journal of Personality and Social Psychology* 82, 3 (2002), 314–327.

[133] Marcel Zeelenberg and Eric van Dijk. 2005. On the comparative nature of regret. In *The Psychology of Counterfactual Thinking*, David R. Mandel, Denis J. Hilton, and Patrizia Catellani (Eds.). Routledge, Abingdon, UK, Chapter 9, 147–162.

[134] Marcel Zeelenberg, Wilco W Van Dijk, Joop Van der Pligt, Antony SR Manstead, Pepijn Van Empelen, and Dimitri Reinderman. 1998. Emotional reactions to the outcomes of decisions: The role of counterfactual thought in the experience of regret and disappointment. *Organizational Behavior and Human Decision Processes* 75, 2 (1998), 117–141.

[135] Xiaolu Zhang, Marcel Zeelenberg, Amy Summerville, and Seger M. Breugelmans. 2021. The role of self-discrepancies in distinguishing regret from guilt. *Self and Identity* 20, 3 (2021), 388–405. https://doi.org/10.1080/15298868.2020.1721316

A SURVEY QUESTIONS

A.1 Demographics

What is your current employment status?

- Employed full-time (not including MTurk)
- Employed part-time (not including MTurk)
- Not employed, looking for work
- Not employed, NOT looking for work
- Student, working at least part-time (not including MTurk)
- Student, NOT working
- Retired

Is using a computer a regular part of your job?

- Yes
- No
- Not Sure

What gender do you most closely identify with?

- Male
- Female
- Non-Binary
- Other:

What is the highest level of education you have obtained?

- Did NOT graduate high school (12th grade or less)
- Graduated high school or equivalent (GED)
- Some college, no degree
- Associate degree
- Bachelor's degree
- Master's degree
- Law degree, M.B.A., or other professional degree
- Doctorate degree

What ethnicity do you primarily identify with?

- Asian/Pacific Islander
- Black/African-American
- White/Caucasian
- Hispanic
- Native American/Alaskan Native/Indigenous
- Other/Multi-Racial
- Prefer not to say

A.2 Regrets from Cybersecurity Experiences in a Professional Setting

Prompt:

People often see how things the past might have been better. You might have acted differently, said something different, and subsequent events might then have unfolded in a better way.

Now think about a cybersecurity experience in your professional life that you regret THE MOST.

What type of cybersecurity experience was this?

- Lost important files, data, or photos
- Work information was compromised
- Lost access to my computer due to malware (e.g., ransomware)
- Clicked on a link in a phishing email
- Responded to a phishing email with confidential information
- My password was compromised and/or used without my permission
- Visited a website that I was not allowed to
- Something else (fill in the blank)
- I have never had a cybersecurity experience in my professional life that I have regretted

Please tell us what happened.

How could of this event have been different?

What makes you see it differently now?

Why do you regret what happened?

What types of cybersecurity, education, training, and/or awareness have you been exposed to by your employer?

Please describe the types of communications and nature of them.

What is a typical example of how they'd communicate to you about cybersecurity, education, training, and/or awareness?

What techniques or strategies do they use to try and make sure you're engaging in safe cybersecurity behavior? (Select ALL that apply!)

- Scare us into compliance
- Explain how certain decisions or actions may lead to undesirable and regretful outcomes
- Provide information on why certain cybersecurity practices are important
- Practice safe cybersecurity behavior through the use of various scenarios
- Send you fake phishing emails to see if you'll click on them
- Tell real stories of how certain actions by others has resulted in compromised cybersecurity
- Other (fill in the blank)