Computers & Security 132 (2023) 103326

Contents lists available at ScienceDirect

Computers & Security

journal homepage: www.elsevier.com/locate/cose

# Cybersecurity Insights Gleaned from World Religions

Karen Renaud[a,b,d,*], Marc Dupuis[c]

[a] University of Strathclyde, Livingstone Tower, Nicholson Street, Glasgow, G11XQ, United Kingdom
[b] University of South Africa, Pretoria, South Africa
[c] University of Washington, Bothell, USA
[d] Abertay University, Dundee, United Kingdom

ARTICLE INFO

*Article history:*
Received 19 December 2022
Revised 19 April 2023
Accepted 5 June 2023
Available online 12 June 2023

*Keywords:*
religion
lessons learned
higher values
socio-technical aspects
sociology

ABSTRACT

Organisations craft and disseminate security policies, encoding the actions they want employees to take to preserve and protect organisational information resources. They engage in regular cybersecurity awareness and training drives to ensure that employees know what to do, and how to do it. Despite these efforts, employees make mistakes or do not comply with policy dictates, triggering cybersecurity incidents. The reality is that whereas cyber professionals propose, human nature disposes.

In addressing this kind of conundrum, researchers suggest that it could be beneficial to learn from the established practices of other domains that also grapple with erratic human behaviours. This seems reasonable, given that cybersecurity is a relatively young field, and not yet particularly successful in accommodating human nature and fallibility, whereas other fields have years of experience coping with these kinds of problems. Here, we consider learning from religions, which have been around for millennia. The one aspect that all understand is human nature, and the tendency of humans to make mistakes and behave ill-advisedly, sometimes despite knowing better. Religions have developed a number of practices to accommodate human frailties, and to care for their adherents. This might well be a fruitful domain for cybersecurity professionals to learn from, in terms of harnessing effective mechanisms to encourage secure behaviours.

To this end, we explored the literature on religions, and interviewed a number of religious leaders to produce a 'vision for cybersecurity'. The vision was evaluated by cybersecurity professionals, its target audience. We provide our vision here, in the hope that it will launch a debate into a more equitable new era of 'best practice' in the cybersecurity domain.



## 1. Introduction

Cybersecurity is a young field of practice whose importance and prominence has grown exponentially over the last two decades. Even so, the number of major cybersecurity incidents continues to be a concern (Anderson et al., 2019). This does not demonstrate overwhelming success in resisting cybercriminals' efforts. In particular, organisations struggle to encourage their employees to follow information security policy dictates. The active policy non-compliance research field (Alqahtani and Braun, 2021; Cram and D'Arcy, 2023; McLeod and Dolezel, 2022) highlights the insufficiency of policies & awareness drives, *on their own*, to guarantee secure behaviours. In addressing this issue, cyber professionals deploy a range of interventions e.g., fear (Renaud and Dupuis, 2019), shaming (Renaud et al. (2021)) and firing employees who cause adverse security incidents (BBC, 2019). These are not universally efficacious, perhaps because organisations lack a strategy that is grounded in a sound knowledge of human nature and values.

Now, consider that more mature fields of practice with centuries-old histories e.g., psychology, medicine and education, are likely to have wrestled with similar challenges and come up with mitigating strategies. As a field matures, one can expect specific interventions and mitigations to have emerged to address challenges (Salafsky and Margoluis, 2003; Travers et al., 2021). These will gradually be refined to improve their ability to address the challenges, or abandoned if they prove ineffective. Younger fields of practice grappling with similar challenges might be able to adopt 'best practice' lessons from these more mature fields, rather

* Corresponding author.
*E-mail address:* karen.renaud@strath.ac.uk (K. Renaud).

https://doi.org/10.1016/j.cose.2023.103326

than having to learn them again, usually by trial and error. Indeed, the Bible's book of Ecclesiastes (1:9) says: "*there is no new thing under the sun*". If true, it seems reasonable for new fields, such as cybersecurity, to improve their success by learning from established fields.

As an example, consider the field of education. Till a few decades ago, teachers regularly beat their pupils, ostensibly to motivate them to learn. Towards the end of the 20th century, enlightenment came, and many countries outlawed physical punishment in schools (Gershoff, 2013). There was a realisation that fear of physical punishment deters learning and exacerbates learning difficulties, quite the opposite of what teachers were trying to achieve. The cybersecurity field still uses fear to scare people into taking precautions (Renaud and Dupuis, 2019), suggesting that they have not yet taken this hard-learned lesson from education on board.

In contemplating which field cybersecurity professionals can learn from to improve their success, we follow De Botton (2012)'s suggestion (echoed by BinTaleb and Aseery (2022); Block et al. (2020)) that secular domains consider which of religions' successful techniques could be appropriated to improve their own success. Religion is certainly much older than cybersecurity, as demonstrated by the age of religious scripts e.g., parts of the Bible are over 3,000 years old (Kugel, 1999). Indeed, Dunbar (2022, p. xi) explains that "*for as long as history has been with us, religion has been a feature of human life*". Religions are certainly successful in gaining and retaining adherents. 'Adherents' is the key word here: they *adhere* to their religion's beliefs and practices. Certainly, many of the world's population adhere to a religion. In 2021, there were an estimated 2.3 billion Christians[1] and 535 million Buddhists[2] worldwide. In 2018, there were 1.8 billion Muslims in the world[3].

Our overarching question is: "*What can cybersecurity learn from religions?*" The **aim** of this paper is to explore this question in order to formulate a vision for organisational cybersecurity, based on these lessons.

Barbour (1997) proposes four ways that 'thinkers' can relate religion and science: (1) conflict, (2) independence, (3) dialogue, and (4) integration. Stenmark (2010) suggests a different typology, whose categories are related to the way these two reconcile with or replace each other. Our focus, here, is on what lessons we can learn from religion. As such, we explore Barbour's concept of *dialogue*: acknowledging that science and religion are distinct but that there is some overlap related to the ways these fields accommodate the foibles of human nature.

Section 2 provides a brief overview of the human-related challenges facing cybersecurity. Section 3 explains why we are proposing to learn lessons from religion. We delineate religion, and then uses Smart (1992)'s and Wilson (1990)'s characterisations to confirm the three cornerstones of religion as modelled by Durkheim (1954), which we use as a structure for our narrative in the rest of this paper. Section 4 then considers what lessons cybersecurity could learn from religions based on the research literature. Section 5 reports on the insights gained from interviews we carried out with religious leaders. Section 6 suggests a vision for cybersecurity informed by the insights we gained, and returns to the research questions we pose in Section 2. In Section 7, we explain how we consulted six cybersecurity professionals, asking them some questions about possible overlaps between religions and cybersecurity, and asking them to give their opinions of our proposed vision. We report on their feedback and suggest directions for future work in Section 8. Section 9 concludes.

[1] https://www.worldatlas.com/articles/largest-religions-in-the-world.html
[2] https://religionmediacentre.org.uk/factsheets/factsheet-buddhism/
[3] https://www.learnreligions.com/worlds-muslim-population-2004480

## 2. Cybersecurity Challenges

All employees need to take cybersecurity-related actions but they do not necessarily all have the same understanding of the risks, and so sometimes make costly mis-steps. Cybersecurity professionals might look upon average users as 'the problem' (Zimmermann and Renaud, 2019): the 'weakest link' (Adams and Sasse, 1999; Ivanov et al., 2021). There is certainly a feeling that end users do not listen to the advice provided by cyber professionals (Ophoff and Renaud, 2021), which puzzles and exasperates them, perhaps explaining why they resort to the use of fear (Renaud and Dupuis, 2019) and shame (Renaud et al., 2021).

Scala et al. (2019) identify "*Five Hard Problems of Cybersecurity*". The fifth is pertinent to this discussion: *understanding and accounting for human behaviour*. This appears to confirm the general feeling that the human tendency to behave insecurely is a somewhat intractable problem, compromising the security of organisational information and devices. Users, on the other hand, often have a variety of reasons for not complying (Ophoff and Renaud, 2021) that make perfect sense to them. For example, some might feel that breaches are inevitable so that compliance is futile (McLeod and Dolezel, 2022), they might have exhausted their compliance budget (Beautement et al., 2008) or they might be *unable* to comply for a variety of reasons (Renaud and Coles-Kemp, 2022).

Given that Koohang et al. (2020) argue that awareness is essential in leading to policy compliance, we will commence by considering awareness drives. What kinds of threats and secure behaviours ought employees to be aware of? Cain et al. (2018) reviewed a number of government websites offering advice, and provide a list of cybersecurity actions that employees are often advised to take. This list includes using hard-to-guess passwords and keeping them private, backing up data and files, and updating applications, software, and operating systems. There is plenty of evidence that these actions are not universally adopted: many still choose weak passwords (Pelchen et al., 2019), do not reliably make backups, and do not want to use two-factor authentication (Dupuis et al., 2019). People also have a tendency to leave their software and devices unpatched (Mathur et al., 2018).

Cain *et al.*'s list of actions is likely too specific and fluid for our purposes in this conceptual discussion. However, Pollini et al. (2021)'s higher level categorisation of human behaviours that compromise cybersecurity appears to offer a viable option to guide our investigations (titles in parentheses ours):

1. **Accidental** and non-deliberate actions resulting in a violation of a security rule (*mistake*).
2. **Deliberate** actions, including: (a) an unintentional violation of a security rule (*negligence*), (b) violations of a security rule with no malicious intent (*non-compliance*), and (c) violations of a security rule with malicious intent (*malice*).

By the end of this paper, we want to be able to answer the following focused research questions:

**RQ1:** Which lessons from religions can help security professionals to reduce employee mistakes?

**RQ2:** Which lessons from religions can help security professionals to prevent deliberate violations of security policies by employees?

## 3. Learning from Other Fields

Very disparate fields can and have learnt from each other. A brief search of the literature reveals many opportunities for cross-fertilisation. For example, Travers et al. (2021) argue that the conservation field could learn lessons from other fields about behavioural change techniques. Salafsky and Margoluis (2003) also address conservation, arguing that they could benefit from

adopting monitoring and evaluation practices from other fields. Sherin et al. (2011) argue that educators could learn from video-based research in other fields. Collie (2003) talks about behavioural telemedicine learning lessons related to communication from other fields. Medicine teaches about the danger of inertia, or being too attached to existing practices (Bown, 2003; Marshall and Warren, 1984) and also about the need to look for systemic causatives when humans make errors (Gawande, 2009).

Cybersecurity professionals have taken inspiration from epidemiology in coping with cybersecurity threats (Modini et al., 2020). We conclude this brief review with a suggestion from Daniel et al. (2020), who argue that construction project management can learn from other fields when it comes to collaboration during project planning. We have mentioned a wide range of divergent fields that, it has been suggested, can learn from each other. The next section explores learning from religions.

### 3.1. Learning from Religions

In terms of other fields learning from religions, others have also made the same arguments as De Botton (2012). For example, BinTaleb and Aseery (2022) ask what the Muslim religion can teach us about pandemics. They identify five themes of wisdom that can inform modern health advice. Block et al. (2020) argue that religion can either encourage or discourage entrepreneurship. DeSteno (2019) argues that religious traditions offer a rich store of insights into human nature and humans' social needs. He also explains that religions use specific techniques to help people to change their views and encourage them to take action. Reich (Reich, 2009, p.225) argues that "*dialogues between science and religion can have positive practical societal relevance*". Finally, Rediehs (2022) suggest a way of integrating science and religion, by focusing on an epistemology that can ground both.

As mentioned in the introduction, religion has evolved over millennia, going through stages, zigzags, and relapses (Ziaowen, 2000). Along the way, they have learnt what works for their adherents, and what does not. This is not to suggest that adherents individually have a direct say in the structure and organisation of a religion or even have the freedom to choose their religion in all cases. Rather, for any institution to remain relevant and thus 'successful', it must in one way or another satisfy the collective over time (Wade, 2009). This is perhaps most evident in both the creation of various denominations and sects of specific religions, as well as clear milestones in the evolution of a particular religion (e.g., the Second Vatican Council in Catholicism). In cybersecurity, professionals are engaging in similar efforts: trying to understand what works to ensure the security of our own and organisations' information resources (Andrade and Yoo, 2019; Friedman, 2013). Similar to religion, cybersecurity will not evolve and change based on any single individual, but instead will evolve when the current system is not working for the collective. It could be argued that the continuing demonstrable success of cybercriminals (AAG, 2023) signals that an evolution is indicated.

### 3.2. Cybersecurity Professionals Learning from Religions

In the cybersecurity domain, cybersecurity professionals:

(1) ***Formulate*** policies that include a range of cybersecurity rules (Li et al., 2019): (a) do *this*, (b) do not do *that*, (c) beware of *the other* (Renaud and Dupuis, 2019).

(2) ***Disseminate*** these via awareness drives (Persadha et al., 2016), and ***test*** awareness (Tempestini et al., 2023).

(3) ***Enforce*** the security rules using a variety of mechanisms, often including sanctions (BBC, 2019). These efforts attempt to ameliorate the impact of human nature on policy compliance (Corradini and Corradini, 2020).

#### 3.2.1. Why the Status Quo Strategy Fails

The rule-based approach fails, as evidenced by the continuing success of cyber criminals AAG (2023), because of:

(1) ***The way cybersecurity rules are formulated***. Some point out that there is little agreement as to the cybersecurity actions employees should be mandated to take (Redmiles et al., 2016; Reeder et al., 2017; Renaud and Weir, 2016). Industry also delivers a similarly divergent range of cybersecurity advice (Brook, 2022; Comm, 2022; Egan and Foreman, 2020; Forbes, 2020; John Egan, 2020; Leaf, 2019; Mitigo and Fleming, 2020; Roesler, 2020; Rubenking and Duffy, 2022). As far as organisations are concerned, Zimmermann and Renaud (2019) point out the inadequacy of security policies, due to the mismatch of policy formulation speed, as opposed to hacker innovation evolution. Moreover, many organisations create rules that are poorly aligned with employees' core jobs (Hart, 2013).

(2) ***The way cybersecurity rules are disseminated***. Security rules are routinely disseminated either in a face-to-face lecture or via an online learning module. Cybersecurity professionals prioritise awareness raising efforts (Corallo et al., 2022; Zhang-Kennedy and Chiasson, 2021), often with an assumption that this will be sufficient to lead to adoption of secure behaviours (Zimmermann and Renaud, 2019). They often test knowledge straight after training efforts (Tempestini et al., 2023). However, despite having attended cybersecurity training, employees might have difficulty remembering the rules (Duncan et al., 2012), or not know how to apply them in their context (Koh, 2019). In this case, awareness does not convert to action.

(3) ***The impact of human nature on secure behaviours.*** Even if we assume that employees know the rules, and know how to act upon them, we have to acknowledge that "*knowing is not the same as doing*" (Wightman and Shakhsheer, 2021) i.e., an employee could well pass a security awareness test, but still not act on their knowledge.

There are likely to be multiple reasons for this 'action paradox'. One might be reactance theory, proposed by Brehm (1966). He explains that when individuals have certain freedoms and these are reduced or threatened with reduction, the individual will work to regain them. Policies restrict freedoms and humans might resent this. This factor has been highlighted by cybersecurity researchers (Lowry et al., 2010; Putri and Hovav, 2014). Another explanation could be that a number of psychological indicators might trigger malicious behaviours (Greitzer and Frincke, 2010). This includes disgruntlement, anger management issues and ignorance of authority, as well as antisocial and narcissistic personalities (Greitzer et al., 2016; Moore et al., 2008; Noonan, 2018). On the other hand, the employee might be stressed or overworked (D'Arcy et al., 2014) or no longer care about the organisation's cybersecurity due to prior bad experiences (Searle and Renaud, 2023). Finally, Reeves et al. (2023) found that employees sometimes became disillusioned with the cybersecurity department's communications, and this would lead them to disregard training.

#### 3.2.2. How Religions Mitigate the Problems

Religions, it turns out, have grappled with these same issues, and found ways to mitigate them.

(1) With respect to ***formulating rules***, each religion has a doctrine, and many have holy books that encode the beliefs and responsibilities of adherents. While there are differences between religions, and even branches of religion (e.g., Catholicism vs. Protestantism), particular communities will generally agree on their particular doctrine and behavioural norms. Hence, over a long period of time, the rules have been agreed and finalised.

(2) With respect to ***disseminating rules***, religions use: (a) repetition, and (b) storytelling. With respect to (a), a religious leader

sermonises at regular meetings: the core principles of their doctrine are disseminated for the edification of attendees – repeating the messages often to ensure that people absorb them. With respect to (b), storytelling is one of the most natural ways in which we communicate and connect with one another (Baker, 2014). Before humans had a written language, storytelling was the primary way humans communicated their history and values across generations (Banks-Wallace, 2002).

It is fundamental to our human nature. According to Hume, "*...poets make use of this artifice of borrowing the names of their persons, and the chief events of their poems, from history, in order to procure a more easy reception for the whole, and cause it to make a deeper impression on the fancy and affection*" (Hume, 2003). In other words, the inclusion of real people and events helps make stories more palatable as it creates a context that they can relate to and more fully appreciate — something religions do well. While storytelling has been a central component of many religions for centuries, the same is not true for organisational communication (Baker, 2014), nor for cybersecurity, even though a number of writers have recently highlighted the power of this practice (Cochran, 2022; Mallory, 2021).

(3) Considering the ***impact of human nature***, we should consider that religions, as a source of morality, attempt to aid in both the exercise of self-control (Rounding et al., 2012) and adoption of pro-social behaviour that benefits society (Norenzayan and Shariff, 2008), in effect helping people to resist their baser instincts (Dewey, 1922). The purpose of morality as provided by religions, then, is to act as a counterbalance to human nature and its resistance to control and constraints. Such benefits may have contributed to the evolution of societies from hunter-gather to agrarian, and so forth (McCullough and Carter, 2011). The problem is that somehow people do not notice their own inconsistencies (Effron and Helgason, 2023), and it could be argued that religions help them to see the consequences of such inconsistencies. Thus, a salient issue to consider is whether similar results related to acknowledging human nature might also inform efforts to influence cybersecurity behaviour in organisations.

### 3.3. Delineating Religion's Dimensions

An understanding of religion's overarching dimensions will provide a structure for the rest of the paper's discussion and the final vision.

#### 3.3.1. Modelling Religion

Durkheim (1954) models religions' three aspects. The religious ***believe***, and their beliefs inform their ***actions***. However, the third integral and crucial part of the equation is the ***belonging*** part. It is 'belonging', and its interactions with 'believing' and 'doing', Haidt (2012) argues, that makes religious communities powerful and effective.

#### 3.3.2. Definitions

In ensuring that we understand religion, it is worth considering definitions. Durkheim defines religion as: "*a unified system of beliefs and practices that unites members into 'one single moral community'* " (Durkheim, 2008, p. 62). Martin (2009) advances a number of definitions of religion, many of which refer to spirituality, faith or the supernatural. The definition that fits best with Durkheim's is: "*communal institutions oriented around a set of beliefs, ritual practices, and ethical or social norms*" (p.163). Bert (2002) simply argues that "*religion relates human beings to spiritual forces beyond their control*". Thoby argues that: "*religion or theology consists of the study of the transcendent or metaphysical*" (Thoby, 2012, p.163).

Here we have four definitions, yet there are many others Willander (2014). Greil (Greil, 2009, p. 247) says: "*It seems safe to assert that no consensus on a definition of religion has been reached and that no consensus is likely to be reached in the foreseeable future*". Grzymala-Busse (2016) cites a number of religious authors e.g., Karen Armstrong (Armstrong, 1996) and Rodney Stark (Stark, 2020), who make the same argument. Hence, we consider a different approach.

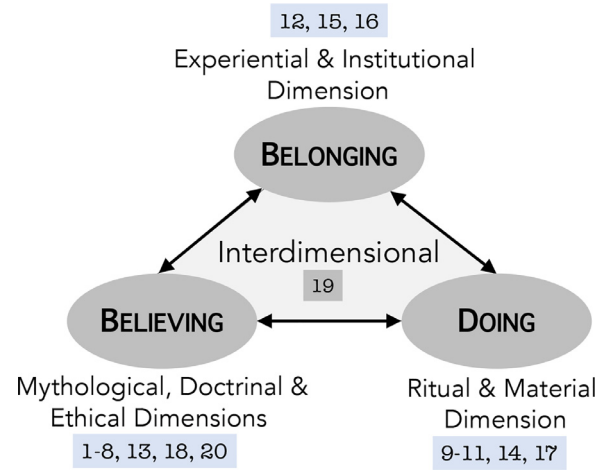


**Fig. 1.** Mapping Durkheim's categories to Smart's Dimensions (Table C.2) and numbers refer to Wilson's Characteristics (Table C.3)

#### 3.3.3. Dimensions

Willander (2014) points to an alternative way of understanding religion, which is to consider its dimensions. He provides a list of seven dimensions that religions exhibit. Using dimensions rather than a definition offers a way to compare fields in a more systematic way. Wilson (1990), on the other hand, provides twenty characteristics that religions exhibit, and pronounce Scientology a religion by showing that it demonstrates these twenty characteristics. Smart also offers a list of dimensions demonstrated by religions (Bishop, 2020). In Table C.3 in the Appendix, we consider which of Wilson's characteristics are aligned with the Durkheim's three aspects and also which of these have been observed in the cybersecurity domain. Fig. 1Fig. 1 maps Durkheim's three religion model aspects to Smart's dimensions and Wilson's characteristics.

### 3.4. Summary

We have shown that it is feasible and meaningful to use Durkheim's three categories to structure our religion-informed vision for cybersecurity, offering a simpler way forward than Wilson's or Smart's more comprehensive sets of characteristics/dimensions. We have discussed two areas that both cybersecurity and religions grapple with, and argue that for these, religions have come up with effective ways to mitigate these problems.

In the next section, we consider the lessons from the research literature related to religion that could meaningfully help cybersecurity professionals.

## 4. Lessons for Cybersecurity from Religion

De Botton (2012) recommends that we take the lessons we need from religion, and apply a measure of creativity in appropriating these for our particular secular domain. This is what we aim to do in this section.

Cybersecurity and religions are not completely dissimilar, confirming the wisdom of using Barbour (1997)'s dialogue approach in carrying out this investigation. For example, both use symbols and

have their own special vocabulary. Religions' symbols are understood by its adherents e.g., 'Star of David' (Judaism) and 'Wheel of Dharma' (Buddhism). The mandala is ubiquitous in Eastern sacred art Krippner (1997). Cybersecurity uses padlocks and keys, hackers with fedora hats and bugs (depicting viruses) (Quinlan et al., 2023).

Both cybersecurity and religions have their own bespoke vocabulary, which outsiders do not necessarily understand. For example, in religion: 'transubstantiation' (Christianty), 'Akaal Takht' (Sikh), 'Ahimsa' (Buddhism, Hinduism and Jainism) and 'Masjid' (Muslim). In cybersecurity, we use the following terms within expert communities: 'HTTPS', 'encryption', 'patching' and 'Zero Day'.

Based on the discussion in the previous section, which shows how Durkheim's model of religious psychology's three interdependent dimensions serve to cover religions' features, we will use this model to structure this discussion (Durkheim, 2008), in considering the lessons cybersecurity can learn from religions.

### 4.1. Belonging

The function and psychology of religions suggests that the great benefit of a well-functioning religion is that it gives adherents a sense of belonging and community (Haidt, 2012). Hence, they make a concerted effort to ensure that new converts feel as if they belong to a religious community of like minded believers. If they do not succeed in making them feel part of the community, it is likely that they will lose them. Religions use a range of techniques to engender this sense of belonging, and have a measure of success due to these techniques being tried and tested.

Christian authors Brand and Yancey (1980) explain that the first sign of civilisation occurs when there is evidence that people help each other; not abandoning those who are going through difficulties. Adler and Barnett (1998) suggest that security communities demonstrate three characteristics: (1) shared identities, values, and meanings; (2) regular meetings; and (3) a sense of responsibility toward one another. Let us now examine each of these in turn

#### 4.1.1. Shared Identities, Values & Meanings

Religions embrace values which become sacred over time (see 'Believing' below), contributing to group identity. Haidt (2012) concludes that humans have evolved to circle around ideas, people and objects. Everyone involved in the religion espouses a core set of ideals and ideas, which is part of their group identity (Pinckney et al., 2021). Some religions, like Christianity, issue daily readings to adherents. Other religions advocate memorisation of their holy scriptures (Islam). This serves to inculcate the shared values and meanings of the religion into the minds of adherents by means of repetition. Meetings, discussed next, serve to reinforce these lessons when the person identifies with a like-minded group that they feel they belong to.

#### 4.1.2. Regular Meetings

*Akrasia* is a Greek word describing the human tendency to know what we should do combined with a perplexing failure to act on our knowledge (Hale and Pillow, 2015; Wiers et al., 2021). Religions acknowledge this, and design a number of ingenuous ways to ameliorate this human tendency to ensure that their adherents do not forget what they ought to do, and to encourage them to act on their knowledge. Many religions emphasise regular meetings Strømsnes (2008) in buildings built and maintained for that purpose e.g., churches, mosques and synagogues. Messages are delivered regularly, during meeting times. Verbal messages are delivered by highly skilled orators. In the words of Cicero, as mentioned by De Botton (2012), those who desire to educate or impact wisdom should seek to *prove*, to *delight* and to *persuade*. Many can attest to the ability of religious ministers to achieve this. Cybersecurity awareness training drives hardly have this reputation (Reeves et al., 2021).

#### 4.1.3. Responsibility to Others

Prinzing (2022) confirms that adherents find a sense of belonging within religious communities. Religions deliberately form supportive communities, with adherents sharing joyous occasions and supporting each other during sad ones (Graham and Haidt, 2010). Many meet regularly with behavioural rules and brands, inspiring loyalty to the community as a whole. Haidt (2012) explains that we are most fulfilled when we operate within a community – a hive, as it were.

Shweder et al. (1997) argue that in collectivist societies there is an ethics of community i.e., authority, respect, duty and loyalty. There is also what they refer to as "*universal cognitions*". Could one of these be the 'Protestant Ethic' that Weber refers to (Weber, 2012), in order to explain how America developed so rapidly in its initial days? We long to become part of something bigger than ourselves and so a secular approach to fulfilling ourselves will inevitably fail. When we pursue our own selfish aims we become unhappy and discontented because we have not evolved for that kind of existence (Comte, 1858). It is interesting to note that cybercriminals have underground forums where they support each other (Afroz et al., 2013).

Haidt (2012) quotes Darwin (1863), who argued that many of our personal virtues benefit those in our communities more than they benefit us personally. Selfish individuals do not cohere and become part of a supportive community, according to Darwin, and their communities are less effective as a consequence. Cybersecurity activities are grounded in notions of individual accountability (van de Poel, 2020; Urquhart and Chen, 2020), as evidenced, for example, by universal prohibitions on sharing of passwords England (2017), and also the way they are indeed shared (Renaud, 2011).

Haidt (2012) argues that when people coalesce into groups they no longer pursue self interest; rather, they pursue the group's interests. Such a community is clearly so much more than the sum of its parts. De Tocqueville (2003) argued that America's strong religious foundations gave it a cooperative power and a competitive force which it would otherwise not have had (cited by Atran (2010)). The immortal words of the poet John Donne Donne, 1642 remind us that we are part of society, something humans need on a very basic level (Perks, 2021; Sharma, 2020).

*No man is an island, Entire of itself;*
*Every man is a piece of the continent, A part of the main.*

### 4.2. Believing

Religious practice is interwoven with believers' lives: they listen to religious music, they admire religious art, they congregate in bespoke locations, they celebrate their life events: births, weddings, and funerals, all with the support of fellow adherents in their religious communities. The person who delivers an oratory eats with the community, visits, and supports adherents during difficult times. The sense of community is strong.

Some people emphasise the fact that religions mandate blind faith (Cook, 1919), and in some respects this is undeniable e.g., virgin birth, transubstantiation and universal salvation. Even so, the Catholic religion specifically encourages its adherents to embrace reason (Woods Jr, 2012). It is perhaps necessary to combine faith with reason: faith in what is taught by experts (Woods Jr, 2012) (sacred values), and reason, where it is possible for people to experience and evidence aspects for themselves. We shall now discuss believing from the perspectives of sacred values, and how the message about these is delivered.

#### 4.2.1. Sacred Values

Religions espouse their own doctrines (Baumard and Boyer, 2013; Christian, 1972; Sutton, 2000), and many have religious texts. These inform the beliefs and behaviours of adherents. How do group ideals and ideas become 'sacred values'? In particular, what is the difference between moral and sacred values? Once considered morally acceptable, through concerted efforts by governments, scientists, and ultimately society, a behaviour or stance may become a moral violation. Moralised attitudes toward a behaviour or action may, over time, develop for an individual, culture, or society. Many behaviours that were once considered a a simple choice, such as smoking, may transform over time through moralisation (Rozin, 1999).

Ryan (2017) explains that moralised attitudes reorient behaviour from maximising gains to adhering to rules. While this is a good first step, people will not feel committed to these values, and may come up with rationalisations not to commit to them (Barlow et al., 2018). Tetlock et al. (2000) says moral values become sacred when they become unviolable and absolute. They explain that whereas people will sometimes trade off between different moral values, sacred values are protected from trade-offs.

Ginges and Atran (2013) find that people will not accept monetary incentives to compromise their sacred values. In religions, the community shares a set of sacred values, which they are committed to. These have to be taught to the community, and then reinforced until they become internalised. Over time they will become sacred. Religion offers some suggestions for the most effective ways of achieving this.

The disagreement between cybersecurity professionals with respect to advisable cybersecurity actions that employees ought to take (Redmiles et al., 2016; Reeder et al., 2017; Renaud and Weir, 2016) is likely to lead to uncertainty, and confirms the relative immaturity of the domain.

#### 4.2.2. Message Delivery

De Botton (2012) argues that 'lessons' should appeal to both reason and emotion if they are going to take hold in the minds of the hearers. It is not enough merely to deliver the facts: it has to be done in such a way that people do not engage in justifying their existing positions. Appealing to emotion is a way of removing defences, if done correctly. The emotion many cyber awareness drives appeal to is fear, and this particular emotion is unlikely to be productive (Renaud and Dupuis, 2019).

With respect to lessons, Leo Tolstoy (Tolstoy, 1894) said: "*The most difficult subjects can be explained to the most slow-witted man if he has not formed any idea of them already; but the simplest thing cannot be made clear to the most intelligent man if he is firmly persuaded that he knows already, without a shadow of doubt, what is laid before him*". Clear (2018) argues that the way to change people's minds is to become their friends, to integrate them into a community: to bring them into your circle. This resonates with Durkheim's idea of 'belonging' and 'believing' being inextricably linked with 'doing'.

Behrens (2022) argues that proselytising religions are the most successful ones. He suggests that proselytizing aligns populations cohesively and makes conversion easier. Indeed, Jackelén (2008) argues that theology has lessons for science in terms of teaching scientists the art of interpreting and understanding difficult concepts.

Using stories to convey lessons is very powerful. Smart (1996) says: "*It is typical of all faiths to hand down vital stories*". Stories, Smart argues, are integrated with the rituals that people engage in. Dr John Rothra (Rothra, 2021), for example, cites a number of mistakes evangelists make: (1) talking *at* people instead of listening to them, (2) presuming that we know other people already know and believe, and (3) denigrating the other person's current lifestyle choices.

Rothra (2014) provides some valuable recommendations for evangelising, which seems appropriate for our purposes too: (1) be an example - walking the walk and not merely talking the talk, and (2) implement small acts of kindness. The first requires us not to tell employees what to do, while doing something different yourself. The second requires us to treat employees kindly when they make mistakes (BBC, 2019), or struggle to behave as they know they ought (Renaud and Coles-Kemp, 2022; Searle and Renaud, 2023).

Campbell and Moyers (2011) argue that humans are spiritual beings, and that this should not be neglected. They argue that: "*One of our problems today is that we are not well acquainted with the literature of the spirit. We're interested in the news of the day and the problems of the hour*" (Campbell and Moyers, 2011, p.13). Humans search for meaning and the way we live our lives, factually, in the here and now, neglects that. Myths, he explains, help us make sense of the world; they satisfy our innate search for meaning and significance. This means that we should weave myths into stories to make them more powerful.

#### 4.2.3. Message Frequency

Many religions emphasise meeting together regularly, during which a message is delivered. Some issue daily readings to ensure regular 'doses' of the core religion's message. Some religions advocate memorisation of their holy texts. Some religions conduct special schools after children's regular schools have finished, to communicate religious values to children.

Now, consider *when* cybersecurity training is currently delivered: very likely when an employee joins the company, annually, or when someone clicks on a Phishing message. Now, consider *how* it is delivered. Many organisations require their employees to complete an online course, and to pass a 'test' to prove that they have understood the content. Undoubtedly they inform, and they might well persuade the person of the need to behave securely. They are not designed to delight the way a sermon often does. Sometimes, employees will attend a face-to-face session. Here, lessons are delivered in a lecture-like situation with someone expounding while using PowerPoint slides from the front of the venue. The approach, again, appeals primarily to the listener's reason, seeking to persuade them of the need to behave securely: to believe in the precepts being imparted by the expert.

In many cases, employees are given so many actions to carry out that they become overwhelmed and give up altogether. Rothra (2021) suggests setting realistic goals. By giving employees realistic goals and slowly adding to the actions they ought to take, we might have a much better chance of their engaging with cybersecurity actions.

#### 4.2.4. Involving all the senses

De Botton argues that religions rely strongly on senses to deliver and emphasise messages De Botton (2012). Many religions like to have feasts, where everyone eats while enjoying the company of others. The East Asian tea ceremony delivers a number of lessons related to many aspects of life – the combination and symbiosis of these conveys lessons far more effectively than mere verbal or textual delivery. In Judaism, on Fridays, the Rabbi leads believers to a ritual bath (the Mikveh). People are asked to forgive those who have wronged them, before getting into the hot and calming bathtub. De Botton (2012) argues that this process maximally benefits from the use of all the person's senses: the comfort that comes from the hot water, the sense of forgiveness being given and grudges being abandoned. Similar traditional activities occur in other religions. For example, Sikhs celebrate Vaisakhi (Singh, 2019), a traditional Punjabi harvest festival celebrated with processions, singing and colourful decorations, appealing to all the senses. Many American Indian ceremonies use peyote, a spineless

cactus that produces psychotropic effects, during religious ceremonies.

Whyte (2017) explains that churches (the buildings), historically, were designed for the ear: to ensure that adherents could hear the preacher. Visual experiences were also accommodated via, for example, stained glass windows. Churches were no longer merely buildings for listening: they now also appealed to the human's visual senses. The Hagia Sophia Mosque built in 360 AD by the Eastern Roman emperor Justinian can also be considered to have been constructed with the idea of appealing to the visual senses.

Mullen (2022) also points to the evocative beauty of the language used in famous hymns, explaining how these titillate the senses e.g., *"Visions of rapture burst on my sight"* (Fanny Jane Crosby, 1873). Recently, a paper was published about the beautification of security ceremonies (Bella et al., 2022), suggesting that this aspect might well also be important in cybersecurity (Quinlan et al., 2023). It is likely the case that we have focused for too long on the technical- and security-related aspects of cybersecurity, and not on the needs of the humans who make use of these systems. Humans are part of the security chain, and they do not *have* to constitute the weakest link (Adams and Sasse, 1999): they can actually be the organisation's strongest weapon in defeating cyber criminals (Zimmermann and Renaud, 2019), but only if we celebrate and acknowledge their humanity.

### 4.3. Doing

This dimension has strong links to 'belonging' and 'believing'. 'Doing' implies acting upon sacred values, which we discuss first. Second, consider the techniques religions use to remind people of the actions to be taken (apart of the teaching aspect, which is part of believing), and finally, the use of rituals to make required actions habitual.

#### 4.3.1. Sacred Values

The importance of these values hs previousl been highlighted under 'Believing' (Section 4.2.1). Jassin et al. (2013) explain that people apply different reasoning to sacred as opposed to secular values. They point out that a sacred value is one that people are entirely committed to: violating the value is unthinkable and non-negotiable. Durkheim (2008) explains that everyone has sacred values. For one person their love for their children is sacred, while for another democracy might be a sacred value (Tumkevič, 2018).

Berns et al. (2012) find that sacred values influence behaviour through the retrieval and processing of deontic rules and not by means of a utilitarian evaluation of costs and benefits during decision making. Atran and Axelrod (2008) explain that sacred values drive action in ways that are not associated with prospects for success. In particular, Shortland (2017) found that when people are faced with two options, the one that involves a sacred value is immediately prioritised.

#### 4.3.2. Reminding: Exhortative, Edifying & Enlightening Art

De Botton (2012) argues that great artists who produce religious art have the ability to inspire and highlight life lessons in a way that is not merely attributable to reason - their aesthetic value communicates with a part of us that reason cannot reach. Tolstoy (1897) confirms, saying "*Art is a human activity having for its purpose the transmission to others of the highest and best feelings to which men have risen*".

De Botton (2012) argues that the purpose of art in the religious world is to: (1) remind you about what is good, and what the good way to live is, and (2) what is bad, unfortunate, sad and unfulfilling. Religious art is didactive and a form of religious propaganda. This begs the question: what would cybersecurity art look like, and what would its purpose be?

We conclude this discussion with two quotes: (1) From Solzhenitsyn (1970) who said: "*Art inflames even a frozen, darkened soul to a high spiritual experience. Through art we are sometimes visited – dimly, briefly – by revelations such as cannot be produced by rational thinking*". (2) From Rebecca West (West, 1941): "*Art is not a plaything, but a necessity, and its essence, form, is not a decorative adjustment, but a cup into which life can be poured and lifted to the lips and be tasted*". It might well be that cybersecurity professionals are missing out on a great tool that could make a real difference in organisations.

#### 4.3.3. Acting: Rituals/Rites/Routines

Values are taught, believed and espoused. The actions that people can take to act upon these values are conveyed to them during message delivery, and ingrained by delivering the message frequently. Religions use habitual rituals and rites, which have a deep spritual significance to their adherents. For example, the Jewish circumcision rite, Navajo sand painting rituals, Mormon baptism of the dead rites and the Christian Eucharist. (Campbell and Moyers, 2011; Durkheim, 2008; Kainz, 2006; Mutter, 2009). Smart (1996) explains that ritualised patterns of behaviour develop a spiritual awareness and ethical insights, DeSteno (2019) explains that ritualistic actions produce effects on the mind which include self-control, feelings of affiliation and empathy for others.

Kligman (1988) discovered, in her anthropological study of rituals in Transylvania, that the agents of the socialist state found it beneficial to build on existing rituals to construct its own traditions. Hence, they did not seek to eradicate religious rituals, but rather to benefit from their existence. Humphrey (1983) also reported the integration of traditional Buryat practices in the organisation of rural Soviet agriculture.

Navajo sacred sand paintings combine rituals with art. These paintings are "*impermanent pictures that serve as temporary ceremonial altars and are a means of attracting powerful supernaturals who are invoked to cure and to bless*" (Parezo, 1981, p. xv). Destroying these paintings is an essential final step of the ritual. Navajo singers use songs, prayers and ritual acts to help individuals to return to 'the Way of Beauty' (McIntosh, 2011).

### 4.4. Summary: Lessons from the Literature

We can now draw out the particular lessons that this review of the literature has to offer the cybersecurity domain:

#### 4.4.1. The Critical Role Played by Sacred Values

Our literature review highlighted the role of sacred values in religion in 'believing', 'belonging' and 'doing'. Yet, Pinckney *et al.* (Pinckney et al., 2021, p.6) explain that "*Sacred values are not necessarily tied to a particular religion or ideology but are simply goals or obligations about which no compromise is possible and to achieve which any sacrifice is acceptable*". Such values are thus not only a religious concept (Lukes, 2017). Gibson (2011) explains that 'sacred' in this sense refers to something priceless and the intrinsically valuable, which seems to map well to the value of personal and organisational information. Bardi and Schwartz (2003) argue that values orient behaviours toward desired goals and outcomes, which, once again resonates with their use in the cybersecurity context. Schwartz (1992) also makes the point that people's values are not context specific and are different from norms, attitudes and specific goals.

In religions, these values are taught, engendering *belief*; they are shared by a community, who circle around the values (Haidt, 2012) (*belonging*); they act in accordance with their shared values (*doing*). We will thus build on this foundational value perspective in

fleshing out our vision of cybersecurity, using the terminology of 'higher values' to reflect the secular nature of our domain.

*4.4.2. Belonging:*

(1) When employees appear negligent or error-prone, it might be that they are depleted or stressed in some way, or that they do not really understand cybersecurity precautions or threats. Managers should be *alert to signs of burnout or confusion* and ct to ameliorate these before a cybersecurity incident occurs as a consequence.
(2) Build a *sense of community* which will support each other when it comes to cybersecurity (Brand and Yancey, 1980). This is likely to mitigate against non-compliance tendencies (Shweder et al., 1997). Moreover, Haidt (2012) argues that *those who belong to a community pursue a common purpose*. Malicious attacks by employees run contrary to this, so ensuring that employees feel they belong to the community is likely to discourage malicious attacks.

*4.4.3. Believing:*

(1) *Shared values should be taught and renewed regularly* (Jassin et al., 2013).
(2) Cybersecurity professionals should *evangelise* employees (Prinzing et al., 2022). This means *being persuasive*, not merely conveying a list of rules and actions to be taken – rather appealing to an agreed set of cybersecurity "shared values" (Wilson, 2018).
(3) When delivering the cybersecurity message, *appeal to the senses* by providing refreshments and background music, and try to make the room attractive (De Botton, 2012; Mullen, 2022). (At the moment, we provide information sessions in dull rooms, we do not use prosaic language, and no one would claim that these experiences are scintillating (Reeves et al., 2021).
(4) Ensure that the message is *heard often*, perhaps when the community comes together for other purposes.
(5) Encourage employees to try to understand the message, by *welcoming questions* (Woods Jr, 2012). Ensure that they understand: (a) why they are being asked to take a particular action, (b) what they ought to do, and (c) how to do it.

*4.4.4. Doing:*

(1) *Encourage adoption of security routines:* something to practice so that it becomes habitual (Lukes, 2017). For example, teach employees to create 'three random word' passwords, and then let them practice this at regular intervals. Moreover, Konvalinka et al. (2011) argue that collective rituals are a deliberate social behaviour. This is especially true when sacred values underlie the ritual (Fisher et al., 2013). The authors also found a link between ritual frequency and group cooperation. The enacting of rituals is thus linked to 'Belonging'.
(2) *The display of cybersecurity art* is likely to remind employees of cybersecurity best practice (De Botton, 2012). For example, consider the poster shown in Fig, 2. By using humour, the creators seek to raise awareness of Phishing. However, it does not explain how to spot a Phish, which seems a missed opportunity. Fig. 2 is not art in any sense, but does deliver a message to the viewer. It is perhaps a first step towards a proxy for art in the cybersecurity domain. Many organisations remind employees of cybersecurity considerations on the lock screens on their computers, or on mouse mats, but it is perhaps worth considering how to make these reminders aesthetically pleasing, as well as informative.
(3) *Employees should be encouraged to ask for support* (link to 'Belonging').
(4) *Employees should be encouraged to ask questions* if they do not understand something (link to 'Believing' & 'Belonging').


**Fig. 2.** Example of a Cybersecurity Poster

## 5. Interviews with Religious Leaders

Given that we're learning from religions, it makes sense to listen to what religious leaders advocate, in terms of accommodating human nature. This part of the research was approved by the University of Strathclyde's Computer and Information Sciences ethical review board. To ensure that we heard from *religions* rather than one specific *religion*, we conducted interviews with an Anglican Priest, a Muslim Scholar, a Buddhist Bhikkhu, a Jewish Rabbi, a Catholic Priest and a Hindu Smaartha Priest.

### 5.1. Interview Process

Participants were recruited via email with contact information for the religious leaders found through various websites after conducting search engine queries.

Semi-structured interviews were employed so that all pertinent topics we sought to explore in the interviews were covered, while also providing flexibility to follow any relevant lines of inquiry based on their responses to questions asked (Krathwohl, 2004). The interviews were conducted using video conferencing software (e.g., Zoom) and lasted approximately 30 minutes each. Permission was granted from the interviewees to record the interviews so that they may later be transcribed for coding and analysis purposes. The recordings were subsequently destroyed once satisfactory transcripts were created. Compensation of $50 USD was offered to US participants for participating. Some opted not to be compensated, others had the compensation directed at their religious institution rather than themselves personally.

### 5.2. Analysis

Our analysis comprised Braun and Clarke (2006) staged thematic analysis: data familiarisation; initial code generation; thematic search and review and defining and naming themes. This offers a way to carry out a systematic yet flexible and accessible way of analysing the data (Braun and Clarke, 2006). The authors analysed the interviews as follows:

1. *Data familiarisation:* Transcribed the interviews, in order to familiarise themselves with the data.
2. *Initial code generation:* Independently coded one of the interviews, then met to agree on a code book.

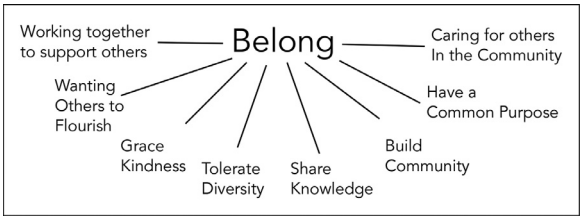


**Fig. 3.** 'Belonging' Themes

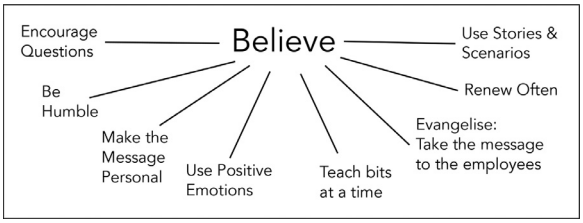


**Fig. 4.** 'Believing' Themes

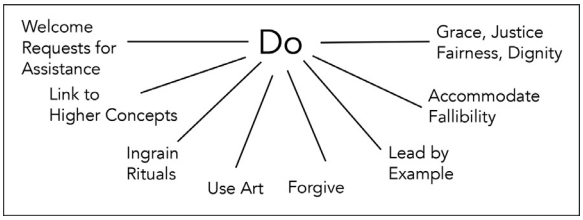


**Fig. 5.** 'Doing' Themes

3. *Thematic search and review:* Coded all the interviews, using the code book. If we needed to add a code, we discussed this before adding it to the code book. We report the inter-rater reliability below.
4. *Defining and naming themes:* Searched for themes, and, in particular, looked for themes that could be categorised under the 'believing', 'belonging' and 'doing' categories.

During this process, we confirmed Durkheim's three overarching themes ('Belonging', 'Believing' and 'Doing'). We then proceeded to identify second order themes, as associated with these overarching categories. The authors met to agree on all themes.

### 5.3. Emerging Themes

Some of the second order themes that emerged from the literature (Section 4.4) were confirmed by this analysis.

#### 5.3.1. Sacred Values

Sacred values were mentioned during the interviews, once again highlighting their crucial role in religions. In our context, it is perhaps more appropriate to talk about *Higher Values*. Indeed, one interviewee referred to higher concepts instead of sacred values during his interview: "*... link us to higher concepts and deeper values*".

Some of the interviewees hint at what the Higher Values could be in cybersecurity. One talks about "*performing one's duties without fail, without anticipation of the outcome*". Another talks about the crucial role of justice: "*everyone has equal access to all resources. Everyone in the community needs to work together to ensure that everyone benefits freely*".

Figs. 3–5 show the themes that emerged within each of Durkheim's categories.

#### 5.3.2. Belonging

This was a strong theme in all of the interviews. One said: "*try to understand each other and realise how much we have in common. We ought not to focus on the differences between us*". Another: "*What is important is community*", with another pointing to our responsibility to "*help other beings*", and to "*strongly wish each one of us to bloom*". One said "*Be there so people can trust you*".

Resonating with the first comment here, one said: "*Difference, difference, difference, but beautifully harmonised*" - emphasising that we are not clones of each other but unique human beings, all of whom can belong to the same community. A statement from a different interviewee agrees: "*It is kind of like a family in a certain sense*".

Finally, one interviewee said "*... so the sense of belonging, the sense of connecting to others, and the sense of being in community is an obligatory kind of staple*". Encouraging employees to ask questions was also a shared theme: "'*ask the questions' because it opens your mind*" and "*... the use of intellect, the use of conversation, dialogue, debate, honing one's own opinions*".

#### 5.3.3. Believing

One interviewee said: "*go out to where the people are rather than just expecting the people to come*" - which describes an evangelising mindset, confirmed by another statement: "*constant renewal that needs to happen... renew and profess; tell a story over and over again*". Stories are essential in conveying concepts: "*The stories are significant to seek knowledge and understanding*" and "*... Stories allow you to open your mind, and compare your trials to those others have experiences*". Questions are encouraged: "*[redacted] is not an absolute unquestioning faith*". Another said that everyone should strive to "*reach enlightenment*".

#### 5.3.4. Doing

The role of rituals emerges: "*Once people have the rhythm down, it is really meant so we don't have to guess what's coming up, rather that we can go through those motions*". Some point to the human need for beauty and explain that religious art attracts people to religion because it satisfies that need: "*and if people are going to be attracted to faith it will in many cases be because of beauty*". Another said: "*art or the aesthetics are a means to an end to better understand and appreciate the core commandments and the core practices*". Finally, another said "*They [art] conveys a simple message in a beautiful way*".

In terms of how we treat people when it comes to their human fallibility and error-prone propensities, one said "*how you behave or act toward another person, hopefully we do so with a sense of how we ourselves would want to be treated or regarded*". Hence, not shaming people Renaud et al. (2021), not scaring them into behaving securely Renaud and Dupuis (2019) and rather forgiving and "*Practice grace - be kind, be forgiving when people make mistakes*". One interviewee referred to their belief in the "*in innate good heart of each person*".

Some referred to the need to acknowledge human fallibility, and say "*Try to make it easier and pleasant for people to behave securely*". Another warned: "*It does not work to scare people into doing things*".

## 6. A Vision for Cybersecurity

It becomes clear, when we consider the lessons from the literature and the insights we obtained from the religious leaders, that everything in religion relies on the espousing and committing to shared values. In cybersecurity, we tend to focus on actions we want employees to take; but the 'values' that we want employees to commit to and espouse are not necessarily articulated nor obvious.

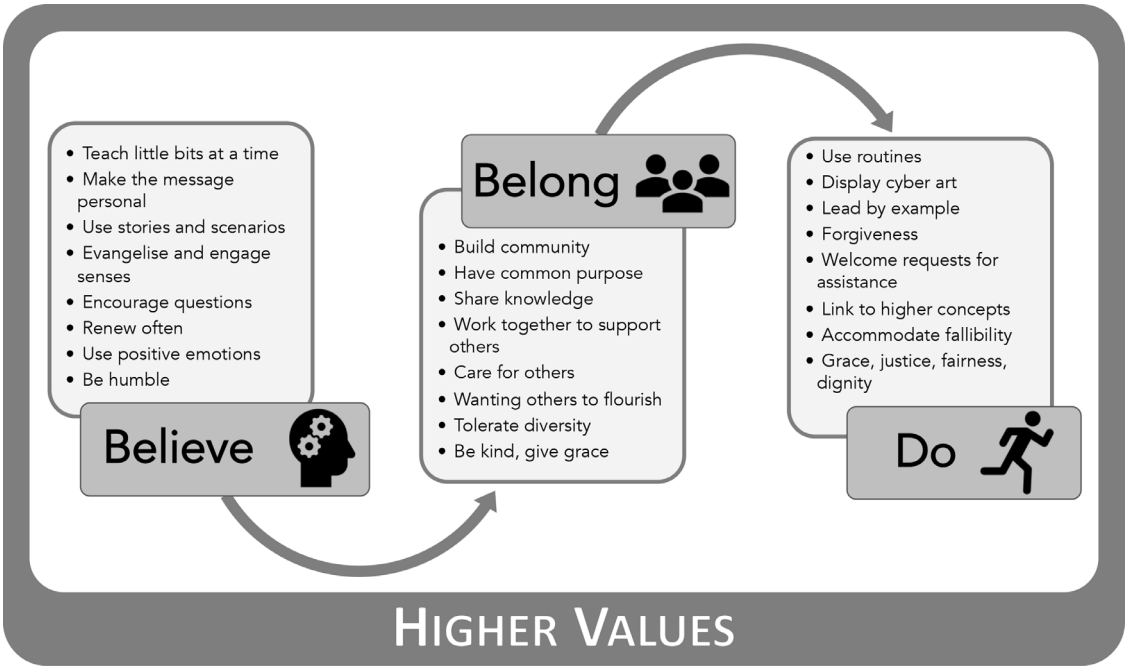


**Fig. 6.** Vision for Cyber Security

Fig. 6 brings together the insights from the research literature and from our interviews to develop a cohesive vision for cybersecurity, which is informed by a shared set of cybersecurity 'Higher Values' (Haidt, 2012).

### 6.1. Cybersecurity Higher Values

Adler and Barnett (1998) highlight the role of a shared set of values in the context of defence and security. Our values do indeed have a powerful influence on our behaviours, informing our decision making and our interpretations of cooperative and competitive behaviours (Sagiv and Schwartz, 2000; Sagiv et al., 2011). This is likely also to apply to cybersecurity. To delineate a set of cybersecurity's higher values is a good topic of future research. However, we briefly discuss some ideas about the topic here, for the sake of completeness.

Dawson and Thomson (2018) suggest that we consider Schwartz et al. (2012)'s values to identify cyber professionals who will be socially aware, and perform better in informing appointment decisions than merely identifying employees who have particular skillsets. They refer to Schwartz et al. (2012) in highlighting the values they consider pertinent. These, while admirable, might, or might not, align with the cybersecurity higher values we want all employees to espouse, as a domain.

Wilson (2018) argues that a myopic focus on a list of preventative actions might be less effective than a focus on cybersecurity values. He does not specify what these individual values should be though. Other authors also talk about cybersecurity values, but do not specifically enumerate what these values are (Marotta and Pearlson, 2019; Yang, 2021), sometimes conflating them with actions they want users to take (Alghenaim et al., 2021). Scala et al. (2019) propose a value hierarchy, but this is more focused on the technical perspective than human shared 'values'.

It might be that cybersecurity values are as simple as the ISO's core information security principles International Standards Organization (2022) of: (1) confidentiality, (2) integrity and (3) availability of information. It is interesting to note that Ibrahim et al. (2014) demonstrate these principles from an Islamic perspective.

van de Poel (2020) identify four cybersecurity values: (1) security, (2) privacy, (3) fairness, and (4) accountability. Christen et al. (2017) also attempted to derive cybersecurity values using a bibliometric approach. They consider the overarching value to be: 'harm prevention'. This does indeed include prevention of harm to information (cybersecurity) as well as physical harm prevention (cybersafety). Huang and Pearlson (2019) also point to the value of 'protecting data'. Christensen *et al.* then add the following to cybersecurity and cybersafety: (1) personal freedom, (2) privacy, (3) social justice, (4) equality, (5) fairness, and (6) discrimination prevention. They also acknowledge that there is potential for tensions between these values.

While cybersecurity professionals could easily commit to these values, we do not know the extent to which individual employees will be able to commit to these relatively broad categories and/or convert them to actions. Nor do we know whether they are effective candidates to serve as the 'higher values' foundation grounding our vision. Investigating this would clearly be a fruitful avenue for future research.

### 6.2. Returning to the Research Questions

We can now return to the research questions and consider how our insights answer these.

**RQ1:** *Which lessons from religions can help security professionals to reduce employee mistakes?*

One of our interviewees specifically mentioned this, saying: "*Practice grace - be kind, be forgiving when people make mistakes*". Others tell us not to wield negative emotions as behavioural control tools (Renaud, 2011; Renaud and Dupuis, 2019; Renaud et al., 2021). Certainly, a sanctions-based response will tend to hurt the individual and the organisation in the long run (Searle and Renaud, 2023). Hence, cybersecurity professionals should make a serious effort to engender a sense of belonging to the cybersecurity community. Employees should be treated as friends and collabora-

tors, which will inform reactions and responses when mistakes are made.

**RQ2:** *Which lessons from religions can help security professionals to prevent deliberate violations of security policies by employees?*

In terms of this aspect of employee behaviour, it seems that the role of a widely-held set of 'higher values' is key, rather than mandating blind adherence to a set of rules (with their currency and aptness being questionable). Consider the fact that some religions *evangelise* converts to bring them into the community, and then emphasise the shared higher values until they, too, espouse these (Wood, 2001). While there may be differences in the details or implementation of these higher values, it is the higher values themselves that can bring people together with a common understanding and purpose.

When employees commit to a set of higher values, negligence is likely to become less of a problem because they are less likely to act selfishly (Haidt, 2012) and will rather pursue the group's interest. Such values become absolute and are protected from trade-offs (Tetlock et al., 2000). Ginges and Atran (2013) argue that people will not compromise the higher values they are committed to, even for monetary incentives. Hence, we need to move from mandating obedience to engendering commitment.

So, to reduce deliberate violations of security rules, we, as the wider cybersecurity community, should first agree upon a set of cybersecurity 'higher values'. We should then use a variety of measures to ensure that everyone believes in them. This will inform employee actions and likely reduce deliberate non-compliance.

## 7. Consulting Experts

To test the viability of our vision, we asked six cybersecurity professionals questions and for their opinion of our vision (See Appendix B). All of the experts worked in companies with more than 500 employees, dealing with their cybersecurity needs.

### 7.1. Experts' Responses

***Which (religious) tools could cybersecurity use?***

A number of these were mentioned, including "*forgiveness for mistakes*", "*the concept of doing the right thing no matter what*", "*reward for doing the right thing and discouraged from doing the wrong thing*". One provided a comprehensive list: (1) Diligence/consistency in rituals (i.e., security practices), 2) Have a doctrine or teaching that is consistent, 3) Go through training and rites of passage that religious people would go through, 4) Go right to the source when something or someone is not practising the correct principles, 5) Innate desire to do good and the right thing, even when nobody is watching (integrity), and 6) Talk about it freely with those around you. A final comment says: "*Cultivating a culture of understanding the security is everyone's responsibility just as believing in your higher power is each individual's "job" that creates a church/religion.*" Many of these are directly included in our vision.

***Meetings***

All agreed with the desirability of meeting regularly, one commenting that it should be voluntary, and another pointing out that it helps to create social bonds in a work environment.

***Rituals/Routines***

Once again, they could see the value of this. One commented: "*Rituals are comforting, normalised, and produce trust and consistency. An example of how to turn something into a ritual would be having a YouTube channel that schedules items of interest every Tuesday at 1PM and eventually may have a way for Admins and others to join in and contribute such as either being on the YouTube show*".

***Community & Belonging***

Once again, all the experts could see the value in this, one commenting "*Well, in an indirect way—yes. Studies have shown that an organisation that fosters a culture of community and belonging tends to have a better cybersecurity posture and improved employee compliance to cybersecurity standards.*" "*This is leadership and people...of which information security department is part of...developing and fostering that culture*".

***Cybersecurity's Higher Values***

A number of values were mentioned by the experts:

1. Protect society, the commonwealth and the infrastructure.
2. Ethical behaviours and not abusing access.
3. Truthfulness.
4. Protecting people.
5. Do the right thing even when nobody is watching.
6. Feel free to blow the whistle if you see something being done incorrectly.
7. Security being everyone's responsibility

***Comments on the Vision***

They were all positive about the general idea of the vision. One commented: "*Great job tying the two entities together through values. People love to strive to be a part of a culture that has a value system where they work for the greater good and in doing so they will succeed.*" Another suggested a wording change: "*I prefer 'practice', 'ceremony', 'ceremonial', 'observance' to 'rituals'*".

***Final Comments***

Although they approved of the vision, some wondered about whether organisations would adopt it: "*This needs buy in and approval from the top of organisations. I would anticipate that main challenges would be the definition of the circumstances in which disciplinary action would be taken as this will never be completely ruled out*". and "*The lessons taken from your interviews hit at the core of the human condition and how to best engage with it. It makes sense that successful and long-lasting religions are ones that are able to distill these practices in positive ways*".

The responses from the experts were positive, which suggests that our vision is a constructive first step towards a better cybersecurity environment within organisations going forward. We know, however, that this is merely a first step. In the next section we highlight some suggestions for future work which will help in advancing this vision.

### 7.2. Comparison of the Vision to Cybersecurity Professionals' Codes of Ethics

A number of codes of ethics exist, and it is helpful to consider how our vision compares to these (Table C.1). A number of principles are mentioned that do not appear in our vision. These generally do not apply to the way the professionals treat others in the organisation, but rather to the way they carry out their own professional duties. e.g., *I will be honest in my professional dealings* (USENIX), *respect for privacy and confidentiality of organisational information, Respect privacy* (ACM), *Honor confidentiality; Maintain and protect the confidentiality of any information* (USENIX). As such, we do not include them in the table.

In conclusion, the codes of ethics are focused primarily on the activities of the cybersecurity professional carrying out their own tasks. As such, they are not particularly informative in terms of how they react to other employees in the organisation, or how they respond to them if an adverse incident occurs. In the 'belong' category, we do see some mention of this, but they do not address the 'believe' category, and the 'do' category is similarly neglected. Hence, there does seem to be a place for our vision to play a role in informing cybersecurity professionals' interactions with employees in organisations.

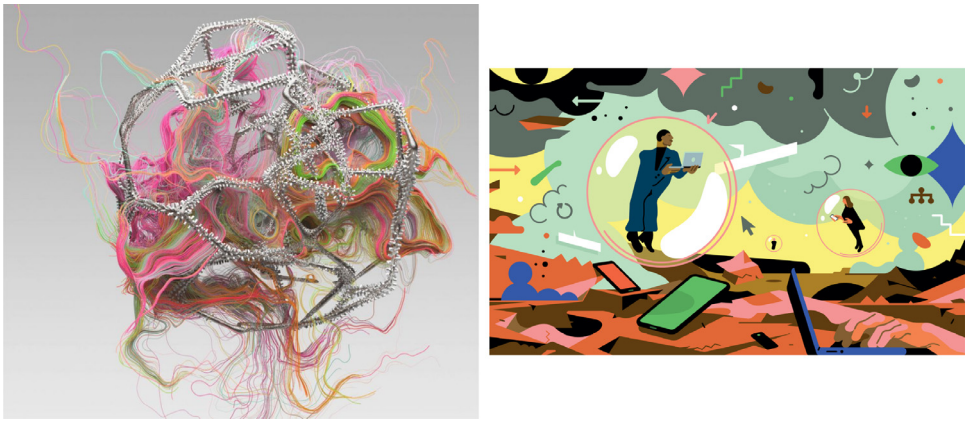

**Fig. 7.** Cybersecurity Art? (Left image from https://brendandawes.com/projects/artofcybersecurity). (The right image is from Kolchoz From Cybersecurity / The Guardian Labs https://www.debutart.com/artist/kolchoz/cybersecurity-the-guardian-labs)

## 8. Future Work

### 8.1. Cybersecurity 'Shared Values'

It is important to investigate the **shared values** that cybersecurity could consider to be 'higher' values that everyone can commit to. Pieters (2011) makes the argument for these values to be the traditional: (1) confidentiality, (2) integrity and (3) availability. While we can see that these might be the values of cybersecurity professionals, there is no evidence that the ordinary computer user would consider these their cybersecurity 'higher values'. Rather than focusing on the minutiae of 'what' people should be doing (rule-based approach), we should identify higher cybersecurity values that people can commit to (the shared values of their community). The secure actions are likely to follow.


**Fig. 8.** 'How To Draw Cyber Security' by Gurzaib Art From https://www.youtube.com/watch?v=kHc7gdOb37I

### 8.2. Cybersecurity Art

Cybersecurity art might be able to perform the same function as religious art: to communicate with the viewer, and to appeal to the senses. The appeal might be aesthetic but it also might be humorous (e.g., Fig. 2). The authors sought in vain for cybersecurity related art, or, for that matter, anything that was remotely aesthetically pleasing. Fig. 7 shows some of the images that were returned when we searched for "*Cybersecurity Art*". The image on the right is somewhat obscure and the left image, while perhaps aesthetically pleasing, does not deliver a message. Neither serves the purpose of art as envisaged by religious artists. Fig. 8, while being *about* cybersecurity, seems merely to confirm the existence of bad actors without giving a specific lesson, and, while illustrative, does not compare to great religious art masterpieces. Consider that the artists who produced religious art were themselves religious e.g. Michelangelo and Leonardo da Vinci. While it is entirely possible for a religious person to be, at the same time, an artist, it occurs to us to wonder how many cybersecurity experts are also artists. This is likely a rarer combination of skills. Pursuing the domain of cybersecurity art would be a particularly good fit for an interdisciplinary team of researchers.

Some work has indeed been undertaken into 'cybersecurity aesthetics'. For example, Bernal (2020) studied three museum exhibits which focus on cybersecurity. She found that the first, called Weapons of Mass Destruction, was designed to instil fear. The second was titled 'Cyber Detectives' and depicted the internet as a mechanical system. The third, 'Covert Operations', aims to shock by highlighting the overreach of surveillance technology. Quinlan et al. (2023) carried out an investigation into the kinds of illustrations used in online cybersecurity reports. They used a web crawler to download 1,027 images that accompanied cybersecurity content online. The authors categorise the images into ten different categories. The most popular one was: "*physical traditional security semiotics (such as lock, key, or shield)*", with the second being "*hackerman archetype*". They discovered colour being used to denote objects as being of specific importance, ranging from useful to dangerous. With respect to the two categories mentioned above, blacks, blues and whites were the most popular colours. This seems to confirm the assertion by Sherin (Sherin et al., 2011, p.82) that "*Cybersecurity experts foster a perception of cybersecurity as a gloomy underworld in which the good guys must resort to unconventional tactics to keep at bay a motley group of threats*". Fig. 8 depicts two 'worlds', good and bad, but it is hard to see what lessons are being provided to viewers.

It is interesting to note that a multitude of aesthetically-pleasing religious art artefacts exist e.g., 'The Last Supper' by Leonardo da Vinci, 'Thangka of Shakyamuni Buddha', 'Great Mosque of Kairouan' in Tunisia, 'The Abode of Nanak' by Granth Sahib, and Marc Chagall's 'Mosaic Window'. These do not focus exclusively on scary topics such as hell and Satan; rather, they seek to titillate the senses and please the eye. On the other hand, we do not see any mention of beauty in any studies of cyber-related illustrations (Quinlan et al., 2023). It seems that the cybersecurity field would benefit from due consideration of the affordances and benefits of aesthetically-pleasing cybersecurity art.

### 8.3. Propositions

Beyond the vision just delineated, the shared higher values may also serve to improve how organisations manage cybersecurity. In this paper, we examined what may be learned from religion and applied to the field of cybersecurity by examining two research questions. The purpose of these research questions was to determine how organisations may best address: (1) mistakes and (2) negligence, non-compliance, and malicious behaviours. Through this examination, we propose two approaches that cybersecurity professionals in organisations may adopt to: 1) more effectively reduce mistakes, and 2) limit negligent, non-compliant, and malicious acts.

#### 8.3.1. Proposition 1: Addressing Mistakes

When mistakes are made, the use of positive over negative emotions will result in comparable or better outcomes for the organisation in the long-term.

#### 8.3.2. Proposition 2: Higher Values and Common Purpose

Organisations that focus on 'higher values' that bring people together with a common understanding and purpose will have fewer incidents of deliberately negligent, non-compliant and malicious behaviours.

## 9. Conclusion

The imperfections of human nature are manifest in our tendencies to make mistakes, be negligent, not comply with rules and occasionally behave maliciously (Hofmann et al., 2014). Religions are centuries old and have developed a number of practices to accommodate human nature. What we sought to do was to appropriate those religious practices that could help cybersecurity to become more successful in addressing these behaviours. We gained insights from the research literature and from religious leaders to derive a vision for cybersecurity. The vision was positively received by consulted cybersecurity professionals. We hope that other researchers will help us to develop and refine our vision to make the vision a truly valuable resource for organisations in dealing with the potentially insecure behaviours of their employees.

## Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

## CRediT authorship contribution statement

**Karen Renaud:** Conceptualization, Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing. **Marc Dupuis:** Methodology, Investigation, Data curation, Writing – original draft, Writing – review & editing.

## Data availability

The data that has been used is confidential.

## Acknowledgements

We thank the religious leaders who were kind enough to speak to us and help us to understand their religions, and to explain the lessons we can learn from them. We thank the six cybersecurity professionals for giving us the benefit of their insights. We thank Rosanne English, Henry Campbell, Jim Hosie, Brian Girvin and Tony Vance for their feedback on an earlier version of this paper.

## Appendix A. Interview Questions

**Introduction:** Religions are centuries old, and cybersecurity is, by comparison, a mere babe in arms. It is important for all fields to learn from more established fields, and we aim to are asking ministers of various religions to help us to understand what we can learn from religion.

**Questions:**

- What kinds of things do you believe your religion emphasises?
- How do you define success for a religion?
- What makes a religion successful?
- What role does symbolism/symbols play within your religion?
- What role does storytelling have within your religion?
- What role do rituals play within your religion?
- What role does art play within your religion?
- What are the top three lessons cybersecurity can learn from your religion?

## Appendix B. Questions for Experts

(1) Both cybersecurity professionals and religious leaders grapple with human nature and their sometimes undesirable behaviours.
(2) Do you think cybersecurity within an organisation could benefit from meeting regularly with employees? If so, what might that look like?
(3) Do you think cybersecurity within an organisation could benefit from developing rituals? If so, what might that look like?
(4) Do you think cybersecurity within an organisation could benefit from a greater emphasis on community and creating a sense of belonging? If so, please explain.
(5) Religions have so-called sacred values - values adherents commit to and will not compromise on. What do you think cybersecurity's higher values are (our secular equivalent of sacred values)?
(6) What practices do you think cybersecurity could borrow from religions to encourage more secure behaviours?
(7) We have spoken to religious leaders, and derived a vision for cybersecurity based on what they told us. You can see our vision in the diagram below. We would love your opinion on this vision. Thanks!

## Appendix C. Tables

**Table C1**
Elements of the Vision in Ethical Codes of Conduct

| VISION | ACM ACM (2022) | USENIX USENIX (2022) | EthicsFirst EthicsFirst (2022) |
|---|---|---|---|
| | | **BELIEVE** | |
| Teach in bits | | | |
| Make message personal | | | |
| Use stories | | | |
| Evangelise & engage senses | | | |
| Encourage questions | | | duty to acknowledge |
| Renew often | | | |
| Use positive emotions | | | |
| Be humble | | | |
| | | **BELONG** | |
| Build community | | | |
| Have common purpose | | | |
| Share knowledge | | share my knowledge and experience with others | duty to inform |
| Work together to support others | contribute to society and to human well-being | be honest and trustworthy | duty of trustworthiness |
| Care for others | ditto | ditto | |
| Want others to flourish | | strive to listen to and understand the needs of all parties | duty to team ability |
| Tolerate diversity | | | |
| Be kind, give grace | avoid harm | build and maintain a safe, healthy, and productive workplace | duty to respect human rights |
| | | **DO** | |
| Use rituals | | | |
| Display cyber art | | | |
| Lead by example | | lead by example | |
| Welcome requests for assistance | | | |
| Link together higher concepts | | | |
| Accommodate fallibility | | | |
| Grace, justice, fairness, forgiveness | be fair and take action not to discriminate | maintain professional conduct in the workplace and not allow personal feelings or beliefs to cause me to treat people unfairly | duty to team health |

**Table C2**
Aspects thought to be shared by Religion and other Domains

| Dimension | Explanation | Other Domains that share features with religions |
|---|---|---|
| | **Durkheim's DOING** | |
| Ritual Dimension | (1) formal rituals (activities with rules surrounding the performance and motivation) Durkheim (2008); Orme (2021), (2) informal, everyday practices (activities with a religious motivation) | Poetry Mutter (2009), Liberalism Kainz (2006), Sport Brody (1979). |
| Material Dimension | Creation of material artefacts, quoted by Cleese in 2018 Cleese (2018), Sharonova et al. (2018); Újvári (2020). | Medicine Raymond (1982), Liberalism has Saints & Martyrs: Kainz (2006), Has a Priesthood & Prophets (Economics, Medicine, Criminology, Liberalism): Haines and Sutton (2000); Kainz (2006); Nelson (2001); Raymond (1982). |
| | **Durkheim's BELIEVING** | |
| Mythological Dimension | The storytelling aspect of religion | Capitalism Thoby (2012), Theatre Bert (2002), Liberalism Kainz (2006), Communication Schultze (2007), Medicine Raymond (1982), Sport Brody (1979), Alcoholics Anonymous Rudy and Greil (1989). |
| Doctrinal Dimension | The way that religions tend to formalise ideas about the world, and create logical systems of meaning Guthrie (1996) | Corporate Governance Kempf (2008), Capitalism Thoby (2012), Symbolism in Sport Fernández and Cachán-Cruz (2017), America Monbiot (2004). |
| Ethical Dimension | Provision of guidance on how to live | Economics Hill (2005), Liberalism Kainz (2006), Economics Nelson (2021), Cyberspace Wertheim (2017), Capitalism Löwy (2009), Communism McFarland (1998), Evolution Ruse (2000), America Monbiot (2004). |

(*continued on next page*)

**Table C2** (*continued*)

| Dimension | Explanation | Other Domains that share features with religions |
|---|---|---|
| | **Durkheim's BELONGING** | |
| Experiential Dimension | Emotions felt by the individual in relation to a religious experiences | Medicine Raymond (1982), Computer Science Williams (2000), Capitalism Löwy (2009), Economics Henry (2002), Alcoholics Anonymous Rudy and Greil (1989). |
| Institutional Dimension | Adherents grouping together, and forming organised bodies that behave collectively | Liberalism Kainz (2006), Theatre Bert (2002), Sport Brody (1979) |
| | **INTERSECTIONAL** | |
| Inter-dimensional travel | Religion occurring at the personal, and collective levels. Including visual, auditory, tactile, dissociative experiences | Worship, creation, ecclesiology, soteriology, eschatology, and divinization Backhouse (2020). |

**Table C3**
Wilson's Characteristics of Religions & Cybersecurity

| # | Characteristic | Religion Ref | Cybersecurity Ref |
|---|---|---|---|
| | | **Durkheim's BELIEVING** | |
| 1 | Belief in an agency(agencies) that transcend normal perception | Henry (2002); Löwy (2009); Raymond (1982); Williams (2000) | Hackers Buchanan (2020) |
| 2 | Belief that the agency influences the natural world and social order | Bert (2002); Thoby (2012) | Social Engineers Salahdine and Kaabouch (2019) |
| 3 | Belief that supernatural intervention in human affairs occurred | | |
| 4 | Belief that supernatural intervention superintends human history | | |
| 5 | Belief that man's fortunes depend on relationships with these supernatural agencies | | Relationships with hackers Seebruck (2015) |
| 6 | Belief that individual destiny can be influenced by their behaviours | Löwy (2009) | Cause and Effect Thinking Dark (2014) |
| 7 | There are prescribed actions for individuals | Similar to Smart's Doctrinal Dimension | Encoded in Security policies Cain et al. (2018) |
| 8 | Individuals can ask supernatural agencies for assistance | | |
| 13 | Moral rules are provided for believers | Similar to Smart's Ethical Dimension | Security Policies Roth et al. (2020) |
| 18 | Required beliefs and actions are systematised and legitimised | Similar to Smart's Doctrinal Dimension | Security Awareness Training efforts deliver this Li et al. (2019) |
| 20 | The claims are accepted as a matter of dogma, as a matter of faith | Blind Faith, as in Liberalism Thoby (2012) citing Fukuyama (2006) and Kempf (2008) | Beliefs Koppel et al. (2016) |
| | | **Durkheim's DOING** | |
| 9 | Symbols of obedience and devotion required in the presence of symbolic representations | | |
| 10 | Designated Language | | Cyber Vocabulary Furnell and Collins (2021) |
| 11 | There are occasions of celebration / mortification | | Incidents lead to mortification Tully et al. (2020); repelling such, joy PhysOrg (2011) |
| 14 | Seriousness of purpose | | Sultan (2022) |
| 17 | Specialist functionaries are paid for services | | Cyber professionals are paid Blažič (2021); De Zan (2019) |
| | | **Durkheim's BELONGING** | |
| 12 | Occasions of worship and exposition of teaching | Similar to Smart's Mythological Dimension | Cyber awareness drives Dash and Ansari (2022) |
| 15 | A moral economy of reward and punishment | Similar to Smart's Ethical Dimension | Person fired for making a mistake BBC (2019) |
| 16 | Custodians of sacred objects exist | Thoby (2012) | Formulation of ENISA as a moral authority Dunn Cavelty and Smeets (2023) |
| | | **Durkheim's BELIEVING & DOING & BELONGING** | |
| 19 | Beliefs, rituals, and institutions | Similar to Smart's Interdimensional; Durkheim (2008); Kainz (2006); Mutter (2009) | Required cyber hygiene actions Cain et al. (2018); Zimmermann and Renaud (2019) |

## References


AAG, 2023. The latest 2023 cyber crime statistics (updated february 2023). Accessed 5 March 2023 https://aag-it.com/the-latest-cyber-crime-statistics/.

Adams, A., Sasse, M.A., 1999. Users are not the enemy. Communications of the ACM 42 (12), 40–46. https://doi.org/10.1145/322796.322806

Adler, E., Barnett, M., 1998. Security Communities. Cambridge University Press, Cambridge.

Afroz, S., Garg, V., McCoy, D., Greenstadt, R., 2013. Honor among thieves: A common's analysis of cybercrime economies. In: APWG eCrime Researchers Summit. IEEE, San Francisco, USA, pp. 1–11. https://doi.org/10.1109/eCRS.2013.6805778

Alghenaim, M.F., Bakar, N.A.A., Yusoff, R.C.M., Hassan, N.H., Sallehudin, H., 2021. Employee awareness model to enhance awareness of social engineering threats in the saudi public sector. In: Proceedings International Congress of Advanced Technology and Engineering (ICOTEN). IEEE, Online, pp. 1–6. https://doi.org/10.1109/ICOTEN52080.2021.9493434

Alqahtani, M., Braun, R., 2021. Reviewing influence of utaut2 factors on cyber security compliance: A literature review. Journal of Information Assurance & Cyber Security 2021, 1–15. http://hdl.handle.net/10453/157514
Anderson, R., Barton, C., Bölme, R., Clayton, R., Ganán, C., Grasso, T., Levi, M., Moore, T., Vasek, M., 2019. Measuring the changing cost of cybercrime. In: Proceedings Workshop on the Economics of Information Security (WEIS). Boston, US, 3-4 June
Andrade, R.O., Yoo, S.G., 2019. Cognitive security: A comprehensive study of cognitive science in cybersecurity. Journal of Information Security and Applications 48, 102352. https://doi.org/10.1016/j.jisa.2019.06.008
Armstrong, K., 1996. Jerusalem: One City Three Faiths. William Collins.
Atran, S., 2010. Talking to the Enemy. Clays Ltd, England.
Atran, S., Axelrod, R., 2008. Reframing sacred values. Negotiation Journal 24 (3), 221–246. https://doi.org/10.1111/j.1571-9979.2008.00182.x
Baker, B., 2014. Use storytelling to engage and align employees around your strategic plans. Industrial and Commercial Training 46 (1), 25–28. https://doi.org/10.1108/ICT-10-2013-0065
Banks-Wallace, J., 2002. Talk that talk: Storytelling and analysis rooted in african american oral tradition. Qualitative Health Research 12 (3), 410–426. https://doi.org/10.1177/104973202129119892
Barbour, I.G., 1997. Religion and Science: 0001 (Gifford Lectures Series). HarperOne; HarperCollins, San Francisco.
Bardi, A., Schwartz, S.H., 2003. Values and behavior: Strength and structure of relations. Personality and Social Psychology Bulletin 29 (10), 1207–1220. https://doi.org/10.1177/0146167203254602
Barlow, J.B., Warkentin, M., Ormond, D., Dennis, A., 2018. Don't even think about it! The effects of antineutralization, informational, and normative communication on information security compliance. Journal of the Association for Information Systems 19 (8), 3. https://aisel.aisnet.org/jais/vol19/iss8/3
Baumard, N., Boyer, P., 2013. Explaining moral religions. Trends in Cognitive Sciences 17 (6), 272–280. https://doi.org/10.1016/j.tics.2013.04.003
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.
Beautement, A., Sasse, M.A., Wonham, M., 2008. The compliance budget: managing security behaviour in organisations. In: Proceedings of the New Security Paradigms Workshop (NSPW), Lake Tahoe, California, USA, pp. 47–58. https://doi.org/10.1145/1595676.1595684
Behrens, A., 2022. What corporations can learn from the struggle in the market for souls. Thunderbird International Business Review 64 (3), 263–265. https://doi.org/10.1002/tie.22258
Bella, G., Ophoff, J., Renaud, K., Sempreboni, D., Viganò, L., 2022. Perceptions of beauty in security ceremonies. Philosophy & Technology 35 (3), 1–34. https://doi.org/10.1007/s13347-022-00552-0
Bernal, V., 2020. The aesthetics of cyber insecurity: Displaying the digital in three American museum exhibits. In: Ghertner, D.A., McFann, H., Goldstein, D.M. (Eds.), Futureproof. Security Aesthetics and the Management of Life. Duke University Press Books, pp. 33–62. https://doi.org/10.1515/9781478007517-003
Berns, G.S., Bell, E., Capra, C.M., Prietula, M.J., Moore, S., Anderson, B., Ginges, J., Atran, S., 2012. The price of your soul: neural evidence for the non-utilitarian representation of sacred values. Philosophical Transactions of the Royal Society B: Biological Sciences 367 (1589), 754–762. https://doi.org/10.1098/rstb.2011.0262
Bert, N.A., 2002. Theatre Is Religion. The Journal of Religion and Theatre 1 (1), 2–12. http://www.rtjournal.org/vol_1/no_1/bert.html
BinTaleb, A., Aseery, A., 2022. What can the prophet muhammad teach us about pandemics? Journal of Religious & Theological Information 21 (1-2), 82–94. https://doi.org/10.1080/10477845.2021.2017552
Bishop, J., 2020. Ninian smart's seven dimensions of religion and why it is helpful. https://jamesbishopblog.com/2020/01/11/ninian-smarts-seven-dimensions-of-religion-and-why-is-it-helpful/.
Block, J., Fisch, C., Rehan, F., 2020. Religion and entrepreneurship: a map of the field and a bibliometric analysis. Management Review Quarterly 70 (4), 591–627. https://doi.org/10.1007/s11301-019-00177-2
Bown, S.R., 2003. Scurvy: How a Surgeon, a Mariner and a Gentleman Solved the Greatest Medical Mystery of the Age of Sail. Summersdale, Chichester, West Sussex.
Brand, P., Yancey, P., 1980. Fearfully and Wonderfully Made. Zondervan, Grand Rapids, Michigan.
Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qualitative Research in Psychology 3 (2), 77–101. https://doi.org/10.1191/1478088706qp063oa
Brehm, J.W., 1966. A theory of psychological reactance. Academic Press, Oxford, UK.
Brook, C., 2022. What is cyber hygiene? a definition of cyber hygiene, benefits, best practices, and more. https://www.digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more Accessed 28 Feb 2023.
Cain, A.A., Edwards, M.E., Still, J.D., 2018. An exploratory study of cyber hygiene behaviors and knowledge. Journal of Information Security and Applications 42, 36–45. https://doi.org/10.1016/j.jisa.2018.08.002
Campbell, J., Moyers, B., 2011. The power of myth. Anchor, USA.
Christen, M., Gordijn, B., Weber, K., van de Poel, I., Yaghmaei, E., 2017. A review of value-conflicts in cybersecurity: A review of value-conflicts in cybersecurity an assessment based on quantitative and qualitative literature analysis. Orbit Journal-An Online Journal for Responsible Research and Innovation in ICT 1 (1), 1–19. https://doi.org/10.29297/orbit.v1i1.28
Christian, W.A., 1972. Oppositions of religious doctrines: A study in the logic of dialogue among religions. Palgrave Macmillan, London.
Clear, J., 2018. Atomic Habits: An Easy and Proven Way to Build Good Habits and Break Bad Ones. Random House, London.
Cochran, C., 2022. Storytelling in cybersecurity. https://www.axonius.com/blog/storytelling-in-cybersecurity.
Collie, K.R., 2003. Interpersonal Communication in Behavioral Telehealth: What Can We Learn from Other Fields? In: Bloom, J.W., Walz, G.R. (Eds.) Cybercounseling & Cyberlearning: An Encore.. CAPS, Incorporated, pp. 345–365. https://eric.ed.gov/?id=ED481147
Comm, J., 2022. 4 actions remote employees can take to improve home cybersecurity. https://www.inc.com/joel-comm/4-actions-remote-employees-can-take-to-improve-home-cybersecurity.html Accessed 28 Feb 2023.
Comte, A., 1858. The positive philosophy of Auguste Comte. Blanchard.
Cook, E.A., 1919. Blind Faith. The Biblical World 53 (2), 173–180. https://doi.org/10.1086/476206
Corallo, A., Lazoi, M., Lezzi, M., Luperto, A., 2022. Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. Computers in Industry 137, 103614. https://doi.org/10.1016/j.compind.2022.103614
Corradini, I., Corradini, I., 2020. Security: human nature and behaviour. Building a Cybersecurity Culture in Organizations: How to Bridge the Gap Between People and Digital Technology 23–47. https://doi.org/10.1007/978-3-030-43999-6_2
Cram, W.A., D'Arcy, J., 2023. Barking Up the Wrong Tree? Reconsidering Policy Compliance as a Dependent Variable within Behavioral Cybersecurity Research. In: Proceedings Hawaii International Conference on System Sciences (HICSS), Hawaii, pp. 4139–4148. https://hdl.handle.net/10125/103137
Daniel, E.I., Pasquire, C., Chinyio, E., Oloke, D., Suresh, S., 2020. Development of collaboration in planning: what can construction project management learn from other fields? In: Proceedings 28th Annual Conference of the International Group for Lean Construction, Berkeley, United States, pp. 289–300. https://doi.org/10.24928/2020/0002
D'Arcy, J., Herath, T., Shoss, M.K., 2014. Understanding employee responses to stressful information security requirements: A coping perspective. Journal of Management Information Systems 31 (2), 285–318. https://doi.org/10.2753/MIS0742-1222310210
Darwin, 1863. The Descent of Man. D Appleton & Co, New York.
Dawson, J., Thomson, R., 2018. The future cybersecurity workforce: going beyond technical skills for successful cyber performance. Frontiers in Psychology 9, 744. https://doi.org/10.3389/fpsyg.2018.00744
De Botton, A., 2012. Religion for Atheists. Penguin, England.
De Tocqueville, A., 2003. Democracy in America, Vol. 10. Penguin Publishing, London, UK.
DeSteno, D., 2019. What science can learn from religion. The New York Times https://www.nytimes.com/2019/02/01/opinion/sunday/science-religion.html.
Dewey, J., 1922. Human nature and conduct. Henry Holt and Company, New York. https://www.gutenberg.org/files/41386/41386-h/41386-h.htm
Donne, J., 1642. No man is an island, entire of itself...https://allpoetry.com/No-man-is-an-island.
Dunbar, R., 2022. How Religion Evolved: And why it Endures. Pelican, UK.
Duncan, J., Schramm, M., Thompson, R., Dumontheil, I., 2012. Task rules, working memory, and fluid intelligence. Psychonomic Bulletin & Review 19, 864–870. https://doi.org/10.3758/s13423-012-0225-y
Dupuis, M., Geiger, T., Slayton, M., Dewing, F., 2019. The use and non-use of cybersecurity tools among consumers: Do they want help? In: Proceedings of the 20th Annual SIG Conference on Information Technology Education, pp. 81–86. https://doi.org/10.1145/3349266.3351419
Durkheim, E., 1954. The elementary forms of the religious life [1912]. Allen & Unwin, UK.
Durkheim, E., 2008. The elementary forms of the religious life. Dover Publications, Mineola, New York. Translated by Swain, Joseph Ward
Effron, D.A., Helgason, B.A., 2023. Moral inconsistency. Advances in Experimental Social Psychology. https://doi.org/10.1016/bs.aesp.2022.11.001In Press
Egan, J., Foreman, D., 2020. 6 cybersecurity tips when you work from home. https://www.forbes.com/advisor/personal-finance/cybersecurity-tips-when-you-work-from-home/, Accessed 28 Feb 2023.
England, L.R., 2017. Is Your Roommate a Felon: Considering the Effect of Criminalizing Password Sharing in Nosal II. SMU Sci. & Tech. L. Rev. 20, 47–60. https://scholar.smu.edu/scitech/vol20/iss1/5
Fanny Jane Crosby, 1873. Blessed assurance. Accessed 5 March 2023 https://www.hymnal.net/en/hymn/h/308.
Fisher, R., Callander, R., Reddish, P., Bulbulia, J., et al., 2013. How do rituals affect cooperation? an experimental field study comparing nine ritual types. Human Nature 24, 115–125. https://doi.org/10.1007/s12110-013-9167-y
Forbes, A., 2020. Smart home cybersecurity explained. https://www.minim.com/blog/smart-home-cybersecurity-explainedAccessed 28 Feb 2023.
Friedman, A.A., 2013. Cybersecurity and trade: National policies, global and local consequences. Center for Technology Innovation at Brookings. https://www.thecre.com/fisma/?p=6922
Gawande, A., 2009. The Checklist Manifesto: How to Get Things Right. Metropolitan Books, London, UK.
Gershoff, E.T., 2013. Spanking and child development: We know enough now to stop hitting our children. Child Development Perspectives 7 (3), 133–137. https://doi.org/10.1111/cdep.12038
Gibson, K., 2011. Making sense of the sacred. Negotiation Journal 27 (4), 477–492. https://doi.org/10.1111/j.1571-9979.2011.00319.x
Ginges, J., Atran, S., 2013. Sacred values and cultural conflict. In: Gelfand, M.J., yue Chiu, C., yi Hong, Y. (Eds.), Advances in Culture and Psychology, Vol. 4. Oxford University Press, New York, NY, pp. 273–301.

Graham, J., Haidt, J., 2010. Beyond beliefs: Religions bind individuals into moral communities. Personality and Social Psychology Review 14 (1), 140–150. https://doi.org/10.1177/1088868309353415
Greil, A.L., 2009. Art: Defining religion. In: Clarke, P., Beyer, P. (Eds.), The World's Religions. Routledge, London, pp. 135–149.
Greitzer, F.L., Frincke, D.A., 2010. Combining traditional cyber security audit data with psychosocial data: towards predictive modeling for insider threat mitigation. In: Probst, C.W., Hunker, J., Gollmann, D., Bishop, M. (Eds.), Insider Threats in Cyber Security. Springer, New York, pp. 85–113. https://doi.org/10.1007/978-1-4419-7133-3
Greitzer, F.L., Imran, M., Purl, J., Axelrad, E.T., Leong, Y.M., Becker, D., Laskey, K.B., Sticha, P.J., 2016. Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk. In: Laskey, K.B., Emmons, I., Costa, P.C.G., Oltramari, A. (Eds.), Proceedings Eleventh International Conference on Semantic Technology for Intelligence, Defense, and Security (STIDS), pp. 19–27. Washington DC, USA
Grzymala-Busse, A., 2016. The difficulty with doctrine: How religion can influence politics. Government and Opposition 51 (2), 327–350. https://doi.org/10.1017/gov.2015.38
Haidt, J., 2012. The Righteous Mind. Penguin, England.
Hale, W.J., Pillow, D.R., 2015. Asymmetries in perceptions of self and others' hypocrisy: Rethinking the meaning and perception of the construct. European Journal of Social Psychology 45 (1), 88–98. https://doi.org/10.1002/ejsp.2064
Hart, W., 2013. Verdraaide Organisaties. Kluwer, Netherlands.
Hofmann, W., Wisneski, D.C., Brandt, M.J., Skitka, L.J., 2014. Morality in everyday life. Science 345 (6202), 1340–1343. https://doi.org/10.1126/science.1251560
Huang, K., Pearlson, K., 2019. For what technology can't fix: Building a model of organizational cybersecurity culture. In: Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS), p. Paper3. http://hdl.handle.net/10125/60074
Hume, D., 2003. A treatise of human nature. Courier Corporation, New York.
Humphrey, C., 1983. Karl Marx Collective: Economy, Society, and Religion in a Siberian Collective Farm. Cambridge University Press, UK.
Ibrahim, J., Ahmed, F., Nuhaabdulaziz, M., Nuha, A., Effra, A., Haqani, A., 2014. Information security in ict from an islamic perspective. International Journal of Science and Research (IJSR) 3 (12), 773–778. https://www.ijsr.net/issue1.php?page=150&i=3&edition=Volume%203%20Issue%2012,%20December%202014
International Standards Organization, 2022. Iso/iec 27001 and related standards information security management. https://www.iso.org/isoiec-27001-information-security.html.
Ivanov, N., Lou, J., Chen, T., Li, J., Yan, Q., 2021. Targeting the weakest link: Social engineering attacks in ethereum smart contracts. In: Proceedings of the ACM Asia Conference on Computer and Communications Security, pp. 787–801. https://doi.org/10.1145/3433210.3453085
Jackelén, A., 2008. What theology can do for science. Theology and Science 6 (3), 287–303. https://doi.org/10.1080/14746700802206941
Jassin, K., Sheikh, H., Obeid, N., Argo, N., Ginges, J., 2013. Negotiating cultural conflicts over sacred values. In: Sycara, K., Gelfand, M., Abbe, A. (Eds.), Models for intercultural collaboration and negotiation. Springer, pp. 133–143. https://doi.org/10.1007/978-94-007-5574-1_6
John Egan, D. F., 2020. 6 cybersecurity tips when you work from home. https://www.securityinfowatch.com/residential-technologies/smart-home/article/21111742/7-tips-for-protecting-smart-home-devices-against-cyberattacks Accessed 28 Feb 2023.
Kainz, H. P., 2006. Liberalism as religion. Touchstone https://epublications.marquette.edu/cgi/viewcontent.cgi?article=1028&context=phil_fac.
Kligman, G., 1988. The wedding of the dead: Ritual, Poetics, and Popular Culture in Transylvania, Vol. 4. Univ of California Press.
Koh, E.H., 2019. Risk management competency development in banks: An integrated approach. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-13-7599-6
Konvalinka, I., Xygalatas, D., Bulbulia, J., Schjødt, U., Jegindø, E.-M., Wallot, S., Van Orden, G., Roepstorff, A., 2011. Synchronized arousal between performers and related spectators in a fire-walking ritual. Proceedings of the National Academy of Sciences 108 (20), 8514–8519. https://doi.org/10.1073/pnas.1016955108
Koohang, A., Anderson, J., Nord, J.H., Paliszkiewicz, J., 2020. Building an awareness-centered information security policy compliance model. Industrial Management & Data Systems 120 (1), 231–247. https://doi.org/10.1108/IMDS-07-2019-0412
Krathwohl, D., 2004. Methods of educational and social science research: an integrated approach, 2 Waveland Press, Long Grove ILL, USA.
Krippner, S., 1997. The role played by mandalas in navajo and tibetan rituals. Anthropology of Consciousness 8 (1), 22–31.
Kugel, J.L., 1999. The Bible as it was. Harvard University Press, USA.
Leaf, 2019. 10 ways to prevent cyber attacks. Accessed 28 Feb 2023, https://leaf-it.com/10-ways-prevent-cyber-attacks/.
Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X., 2019. Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. International Journal of Information Management 45, 13–24. https://doi.org/10.1016/j.ijinfomgt.2018.10.017
Lowry, P.B., Teh, N., Molyneux, B., Bui, S.N., 2010. Using theories of formal control, mandatoriness, and reactance to explain working professionals' intent to comply with new it security policies. In: Proceedings Dewald Roode Workshop on Information Systems Security Research, Boston, MA, USA.
Lukes, S., 2017. Sacred values in secular politics. Analyse & Kritik 39 (1), 101–118. https://doi.org/10.1515/auk-2017-0006
Mallory, P., 2021. Storytelling in cybersecurity: The impact of a great story (with sarah moffatt). https://resources.infosecinstitute.com/topic/infosec-inspire-presents-storytelling-in-cybersecurity-the-impact-of-a-great-story-with-sarah-moffatt/.
Marotta, A., Pearlson, K., 2019. A culture of cybersecurity at banca popolare di sondrio. In: Proceedings 25th Americas Conference on Information Systems, Cancun, p. Paper24. https://aisel.aisnet.org/amcis2019/info_security_privacy/info_security_privacy/24
Marshall, B., Warren, J.R., 1984. Unidentified curved bacilli in the stomach of patients with gastritis and peptic ulceration. The Lancet 323 (8390), 1311–1315. https://doi.org/10.1016/S0140-6736(84)91816-6
Martin, C., 2009. Delimiting religion. Method & Theory in the Study of Religion 21 (2), 157–176. https://doi.org/10.1163/157006809X431015
Mathur, A., Malkin, N., Harbach, M., Peer, E., Egelman, S., 2018. Quantifying users' beliefs about software updates. In: Proceedings Workshop on Usable Security (USEC), 18 February, San Diego, CA, USA, pp. 1–7. https://doi.org/10.14722/usec.2018.23036
McCullough, M.E., Carter, E.C., 2011. Waiting, tolerating, and cooperating: Did Religion Evolve to Prop Up Humans' Self Control Abilities. In: Baumeister, R., Vohs, K. (Eds.), Handbook of self-regulation: Research, theory, and applications. Guilford Press, pp. 422–440.
McIntosh, K. H., 2011. Looking beyond the self: Tibetan buddhist and navajo transformation ceremonies. Seminar, Religious Studies Senior.
McLeod, A., Dolezel, D., 2022. Information security policy non-compliance: Can capitulation theory explain user behaviors? Computers & Security 112, 102526. https://doi.org/10.1016/j.cose.2021.102526
Mitigo, Fleming, D., 2020. Cybersecurity when working from home. https://www.lawsociety.org.uk/topics/small-firms/cybersecurity-when-working-from-home Accessed 28 Feb 2023.
Modini, J., Lynar, T., Sitnikova, E., Joiner, K., 2020. Applications of epidemiology to cybersecurity. In: Proceedings European Conference on Cyber Warfare and Security. Academic Conferences International Limited, pp. 483–490. https://doi.org/10.34190/EWS.20.057
Moore, A.P., Cappelli, D.M., Trzeciak, R.F., 2008. The "big picture" of insider IT sabotage across US critical infrastructures. In: Stolfo, S.J., Bellovin, S.M., Keromytis, A.D., Hershkop, S., Smith, S.W. (Eds.), Insider Attack and Cyber Security. Springer, pp. 17–52. https://doi.org/10.1007/978-0-387-77322-3_3
Mullen, P., 2022. Things I never knew about churches. Accessed 1 March 2023 https://www.conservativewoman.co.uk/things-i-never-knew-about-churches/.
Mutter, M.D., 2009. Poetry against religion, poetry as religion: Secularism and its discontents in literary modernism. Yale University.
Noonan, C. F., 2018. Spy the Lie: Detecting Malicious Insiders. Pacific Northwest National Lab.(PNNL), Richland, WA (United States). Prepared for the US Department of Energy.
Norenzayan, A., Shariff, A.F., 2008. The origin and evolution of religious prosociality. Science 322 (5898), 58–62. doi:10.1126/science.1158757.
Ophoff, J., Renaud, K., 2021. Revealing the cyber security non-compliance "attribution gulf". In: Proceedings Hawaii International Conference on System Sciences (HICSS). University of Hawaii at Manoa, pp. 4557–4566.
Parezo, N.J., 1981. NAVAJO SANDPAINTINGS: FROM RELIGIOUS ACT TO COMMERQAL ART. Anthropology.
Pelchen, C., Jaeger, D., Cheng, F., Meinel, C., 2019. The (persistent) threat of weak passwords: Implementation of a semi-automatic password-cracking algorithm. In: Proceedings International Conference on Information Security Practice and Experience. Springer, pp. 464–475. https://doi.org/10.1007/978-3-030-34339-2_27
Perks, M.E., 2021. Self-isolated but not alone: community management work in the time of a pandemic. Leisure Sciences 43 (1-2), 177–183. https://doi.org/10.1080/01490400.2020.1773999
Persadha, P.D., Waskita, A., Fadhila, M., Kamal, A., Yazid, S., 2016. How inter-organizational knowledge sharing drives national cyber security awareness?: A case study in indonesia. In: Proceedings 18th International Conference on Advanced Communication Technology (ICACT). IEEE, pp. 550–555. https://doi.org/10.1109/ICACT.2016.7423468
Pieters, W., 2011. The (social) construction of information security. The Information Society 27 (5), 326–335. https://doi.org/10.1080/01972243.2011.607038
Pinckney, J., Niconchuk, M., Ryan, S., 2021. Motives, benefits, and sacred values. United States Institute of Peace https://link.bowdoin.edu/portal/Motives-benefits-and-sacred-values--examining/6FKgCv2zltg/.
van de Poel, I., 2020. Core values and value conflicts in cybersecurity: beyond privacy versus security. In: Christen, M., Gordijn, B., Loi, M. (Eds.), The Ethics of Cybersecurity. Springer, pp. 45–72. https://doi.org/10.1007/978-3-030-29053-5_3
Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., Guerri, D., 2021. Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work 24, 371–390. https://doi.org/10.1007/s10111-021-00683-y
Prinzing, M., Van Cappellen, P., Fredrickson, B.L., 2022. More than a momentary blip in the universe? investigating the link between religiousness and perceived meaning in life. Personality and Social Psychology Bulletin. https://doi.org/10.1177/01461672211060136
Prinzing, M. M., 2022. Religion gives life meaning. can anything else take its place?Accessed 3 March 2023 https://psyche.co/ideas/religion-gives-life-meaning-can-anything-else-take-its-place.
Putri, F.F., Hovav, A., 2014. Employees compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory.

In: European Conference on Information Systems (ECIS), Tel Aviv, Israel, June 9-11, pp. 1–17. http://aisel.aisnet.org/ecis2014/proceedings/track16/2
Quinlan, K., Cross, A., Simpson, A, 2023. The Aesthetics of Cyber Security: How do Users Perceive Them? https://doi.org/10.48550/arXiv.2306.08171.
Rediehs, L., 2022. The quaker experiential integration of science and religion. Theology and Science 20 (2), 138–155. https://doi.org/10.1080/14746700.2022.2051247
Redmiles, E.M., Kross, S., Mazurek, M.L., 2016. How I learned to be secure: a census-representative survey of security advice sources and behavior. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security, pp. 666–677. https://doi.org/10.1145/2976749.2978307
Reeder, R.W., Ion, I., Consolvo, S., 2017. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. IEEE Security & Privacy 15 (5), 55–64. https://doi.org/10.1109/MSP.2017.3681050
Reeves, A., Calic, D., Delfabbro, P., 2021. “Get a red-hot poker and open up my eyes, it’s so boring” 1: Employee perceptions of cybersecurity training. Computers & Security 106, 102281. https://doi.org/10.1016/j.cose.2021.102281
Reeves, A., Calic, D., Delfabbro, P., 2023. ‘generic and unusable’: Understanding employee perceptions of cybersecurity training and measuring advice fatigue. Computers & Security. https://doi.org/10.1016/j.cose.2023.103137
Reich, K.H., 2009. Progress with science and religion issues: Critical questions and suggestions. Theology and Science 7 (3), 225–244. https://doi.org/10.1080/14746700903036478
Renaud, K., 2011. Blaming noncompliance is too convenient: What really causes information breaches? IEEE Security & Privacy 10 (3), 57–63. https://doi.org/10.1109/MSP.2011.157
Renaud, K., Coles-Kemp, L., 2022. Accessible and inclusive cyber security: a nuanced and complex challenge. SN Computer Science 3 (5), Paper346. https://doi.org/10.1007/s42979-022-01239-1
Renaud, K., Dupuis, M., 2019. Cyber security fear appeals: Unexpectedly complicated. In: Proceedings of the New Security Paradigms Workshop (NSPW), Costa Rica, pp. 42–56. https://doi.org/10.1145/3368860.3368864
Renaud, K., Searle, R., Dupuis, M., 2021. Shame in cyber security: effective behaviour modification tool or counterproductive foil? In: Proceedings New Security Paradigms Workshop (NSPW), Online, pp. 70–87. https://doi.org/10.1145/3498891.3498896
Renaud, K., Weir, G.R., 2016. Cybersecurity and the unbearability of uncertainty. In: Proceedings Cybersecurity and Cyberforensics Conference (CCC). IEEE, pp. 137–143. https://doi.org/10.1109/CCC.2016.29
Roesler, M., 2020. Working from home? here’s what you need for a secure setup. https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup Accessed 28 Feb 2023.
Rothra, J., 2014. A review of seven common evangelism methods. Accessed 5 March 2023 https://www.johnrothra.com/share/evangelism/review-seven-common-evangelism-methods/.
Rothra, J., 2021. Evangelism is the mission of the church. evangelism is the mission of every follower of jesus. however, we don’t always do it right. Accessed 5 March 2023 https://www.johnrothra.com/share/evangelism/six-ways-to-do-evangelism-wrong/.
Rounding, K., Lee, A., Jacobson, J.A., Ji, L.-J., 2012. Religion replenishes self-control. Psychological Science 23 (6), 635–642. doi:10.1177/0956797611431987.
Rozin, P., 1999. The process of moralization. Psychological Science 10 (3), 218–221. https://doi.org/10.1111/1467-9280.0013
Rubenking, N. J., Duffy, J., 2022. 12 simple things you can do to be more secure online. https://uk.pcmag.com/antivirus/94680/12-simple-things-you-can-do-to-be-more-secure-online Accessed 28 Feb 2023.
Ryan, T.J., 2017. No compromise: Political consequences of moralized attitudes. American Journal of Political Science 61 (2), 409–423. https://doi.org/10.1111/ajps.12248
Sagiv, L., Schwartz, S.H., 2000. Value priorities and subjective well-being: Direct relations and congruity effects. European Journal of Social Psychology 30 (2), 177–198. https://doi.org/10.1002/(SICI)1099-0992(200003/04)30:2⟨177::AID-EJSP982⟩3.0.CO;2-Z
Sagiv, L., Sverdlik, N., Schwarz, N., 2011. To compete or to cooperate? values’ impact on perception and action in social dilemma games. European Journal of Social Psychology 41 (1), 64–77. https://doi.org/10.1002/ejsp.729
Salafsky, N., Margoluis, R., 2003. What conservation can learn from other fields about monitoring and evaluation. BioScience 53 (2), 120–122. https://doi.org/10.1641/0006-3568(2003)053[0120:WCCLFO]2.0.CO;2
Scala, N.M., Reilly, A.C., Goethals, P.L., Cukier, M., 2019. Risk and the five hard problems of cybersecurity. Risk Analysis 39 (10), 2119–2126. https://doi.org/10.1111/risa.13309
Schwartz, S.H., 1992. Universals in the content and structure of values: Theoretical advances and empirical tests in 20 countries. In: Zanna, M.P. (Ed.), Advances in Experimental Social Psychology, Vol. 25. Elsevier, pp. 1–65. https://doi.org/10.1016/S0065-2601(08)60281-6
Schwartz, S.H., Cieciuch, J., Vecchione, M., Davidov, E., Fischer, R., Beierlein, C., Ramos, A., Verkasalo, M., Lönnqvist, J.-E., Demirutku, K., Dirilen-Gumus, Ozlem Konty, M., 2012. Refining the theory of basic individual values. Journal of Personality and Social Psychology 103 (4), 663–688. https://doi.org/10.1037/a0029393
Searle, R., Renaud, K., 2023. Trust and vulnerability in the cybersecurity context. In: Proceedings Hawaii International Conference on System Sciences (HICSS), Maui, Hawaii, pp. 5228–5240.
Sharma, A., 2020. Finding community during a pandemic. Science 368 (6487). 206–206, https://doi.org/10.1126/science.368.6487.206
Sherin, M., Jacobs, V., Philipp, R., 2011. Situation awareness in teaching: What educators can learn from video-based research in other fields. In: Sherin, M., Jacobs, V., Philipp, R. (Eds.), Mathematics Teacher Noticing. Routledge, pp. 81–95. https://doi.org/10.4324/9780203832714
Shortland, N.D., 2017. Conflict: sacred values, decision inertia and the psychology of choice in military decision-making. Institute of Psychology, Health and Society.
Shweder, R.A., Much, N.C., Mahapatra, M., Park, L., 1997. The ”big three” of morality (autonomy, community, divinity) and the ”big three” explanations of suffering. Taylor & Frances/Routledge.
Singh, J., 2019. Factsheet: Vaisakhi. Accessed 5 March 2023 https://religionmediacentre.org.uk/factsheets/sikh-vaisakhi/.
Smart, N., 1992. The World’s Religion. Cambridge: Cambridge University Press.
Smart, N., 1996. Dimensions of the sacred: An anatomy of the world’s beliefs. Univ of California Press.
Solzhenitsyn, A., 1970. Nobel lecture. https://www.nobelprize.org/prizes/literature/1970/solzhenitsyn/lecture/.
Stark, R., 2020. The Rise of Christianity: A Sociologist Reconsiders History. Princeton University Press.
Stenmark, M., 2010. Ways of Relating Science and Religion. In: Harrison, P. (Ed.), The Cambridge Companion to Science and Religion. Cambridge University Press, pp. 278–295.
Strømsnes, K., 2008. The importance of church attendance and membership of religious voluntary organizations for the formation of social capital. Social Compass 55 (4), 478–496. https://doi.org/10.1177/0037768608097234
Sutton, N., 2000. Religious doctrines in the Mahābhārata. Motilal Banarsidass Publ., Delhi.
Tempestini, G., Rovira, E., Pyke, A., Di Nocera, F., 2023. The Cybersecurity Awareness INventory (CAIN): Early Phases of Development of a Tool for Assessing Cybersecurity Knowledge Based on the ISO/IEC 27032. Journal of Cybersecurity and Privacy 3 (1), 61–75. https://doi.org/10.3390/jcp3010005
Tetlock, P.E., Kristel, O.V., Elson, S.B., Green, M.C., Lerner, J.S., 2000. The psychology of the unthinkable: taboo trade-offs, forbidden base rates, and heretical counterfactuals. Journal of Personality and Social Psychology 78 (5), 853–870. https://doi.org/10.1037/0022-3514.78.5.853
Thoby, A., 2012. Capitalism as religion. The Student Economic Review 26, 161–171. https://www.tcd.ie/Economics/SER/past-issues/2012.php
Tolstoy, L., 1894. The kingdom of God is within you. William Heinemann, London. Translated by A Delano
Tolstoy, L., 1897. What is Art?, London. Translated by Aylmer Maude
Travers, H., Walsh, J., Vogt, S., Clements, T., Milner-Gulland, E., 2021. Delivering behavioural change at scale: What conservation can learn from other fields. Biological Conservation 257, 109092. https://doi.org/10.1016/j.biocon.2021.109092
Tumkevič, A., 2018. Uncertain security community: Building western cyber-security order. Journal of Information Warfare 17 (1), 74–86. https://www.jstor.org/stable/26504130
Urquhart, L., Chen, J., 2020. On the principle of accountability: Challenges for smart homes & cybersecurity. In: Crabtree, A., Haddadi, H., Mortier, R. (Eds.), Privacy by Design for the Internet of Things. Institution of Engineering and Technology, pp. 19–47. https://doi.org/10.48550/arXiv.2006.11043
Wade, N., 2009. The faith instinct: How religion evolved and why it endures. Penguin, New York.
Weber, M., 2012. The Protestant ethic and the spirit of capitalism. Renaissance Classics, USA.
West, R., 1941. Black Lamb and Grey Falcon. The Record of a Journey Through Yugoslavia. The Viking Press.
Whyte, W., 2017. Unlocking the Church: the lost secrets of Victorian sacred space. Oxford University Press, Oxford.
Wiers, R.W., van Gaal, S., Le Pelley, M.E., 2021. Akrasia and addiction: Neurophilosophy and psychological mechanisms. In: Harbecke, J., Hermann-Pillath, C. (Eds.), Social Neuroeconomics. Routledge, Oxford, UK, pp. 121–147.
Wightman, S.C., Shakhsheer, B.A., 2021. Informed decision-making: Knowing is not the same as doing. Journal of the American College of Surgeons 233 (4), 578–579. https://doi.org/10.1016/j.jamcollsurg.2021.06.009
Willander, E., 2014. What counts as religion in sociology? The problem of religiosity in sociological methodology. Sociologiska institutionen.
Wilson, B.R., 1990. The social dimensions of sectarianism: Sects and new religious movements in contemporary society. Clarendon Press, Oxford.
Wilson, R.E., 2018. Cybersecurity growth program. In: Barker, K., Berry, D., Rainwater, C. (Eds.), Proceedings IIE Annual Conference. Proceedings Institute of Industrial and Systems Engineers (IISE), Orlando, Florida, pp. 1811–1815.
Wood, I.N., 2001. The missionary life. Saints and the Evangelisation of Europe, 400-1050. Routledge, London.
Woods Jr, T., 2012. How the Catholic Church built Western Civilization. Regnery Publishing, Washington, USA.
Yang, Y., 2021. Construction of network security law enforcement virtual simulation experiment and teaching platform. In: Proceedings 6th International Conference on Education Reform and Modern Management (ERMM). Atlantis Press, pp. 152–156. https://doi.org/10.2991/assehr.k.210513.036
Zhang-Kennedy, L., Chiasson, S., 2021. A systematic review of multimedia tools for cybersecurity awareness and education. ACM Computing Surveys (CSUR) 54 (1), 1–39. https://doi.org/10.1145/3427920
Ziaowen, Y., 2000. China’s current religious question: Once again, an inquiry into the five characteristics of religion. Chinese L. & Gov’t 33, 75–100. https://doi.org/10.2753/CLG0009-4609330275

Zimmermann, V., Renaud, K., 2019. Moving from a 'human-as-problem' to a 'human-as-solution' cybersecurity mindset. International Journal of Human-Computer Studies 131, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

**Karen Renaud** is a Scottish computing Scientist at the University of Strathclyde in Glasgow, working on all aspects of Human-Centred Security and Privacy. She was educated at the Universities of Pretoria, South Africa and Glasgow. She is particularly interested in deploying behavioural science techniques to improve security behaviours, and in encouraging end-user privacy-preserving behaviours. She collaborates with academics in 5 continents and incorporates findings and techniques from multiple disciplines in her research.

**Marc J. Dupuis**, Ph.D., is an Associate Professor within the Computing and Software Systems Division at the University of Washington Bothell. Dr. Dupuis earned a Ph.D. in Information Science at the University of Washington with an emphasis on cybersecurity. Prior to this, he earned an M.S. in Information Science and a Master of Public Administration (M.P.A.) from the University of Washington, as well as an M.A. in Political Science at Western Washington University. His research area is cybersecurity with an emphasis on the human factors of cybersecurity. The primary focus of his research involves the examination of psychological traits and their relationship to the cybersecurity and privacy behavior of individuals. This has included an examination of antecedents and related behaviors, as well as usable security and privacy. His goal is to both understand behavior as it relates to cybersecurity and privacy, and discover what may be done to improve that behavior. More recently, Dr. Dupuis and his collaborators have been exploring the use of fear appeals, shame, and regret in cybersecurity, including issues related to their efficacy and the ethics of using such techniques to engender behavioral change. He has a strong track record of multi-disciplinary research, including serving as the principal investigator for a team with an economist, lawyer, and computer scientists. He has published in a broad range of venues, reflecting his multi-disciplinary approach to cybersecurity and privacy. Dr. Dupuis has been involved with the University of Washington's tri-campus Center for Information Assurance and Cybersecurity (CIAC). He has also been nominated for both the Distinguished Research, Scholarship, and Creative Activities Award and the Distinguished Teaching Award at UW Bothell; the highest honors in research and teaching, respectively.