DE GRUYTER Homeland Security & Emergency Management 2014; 11(4): 489–510

Shari Lawrence Pfleeger*, M. Angela Sasse and Adrian Furnham

From Weakest Link to Security Hero: Transforming Staff Security Behavior

Abstract: Practitioners, researchers and policy-makers involved with cyber security often talk about "security hygiene:" ways to encourage users of computer technology to use safe and secure behavior online. But how do we persuade workers to follow simple, fundamental processes to protect themselves and others? These issues are raised by behavioral scientists, to encourage worker, passenger and patient compliance. In this paper, we explore and summarize findings in social psychology about moral values and habit formation, and then integrate them into suggestions for transforming staff security behavior online.

Keywords: behavior change; habit formation; moral dimensions; security hygiene.

DOI 10.1515/jhsem-2014-0035

1 Introduction

Practitioners, researchers and policy-makers involved with cyber security often talk about "security hygiene:" ways to encourage users of computer technology to use safe and secure behavior online. There is significant evidence that current security awareness activities are not effective. For example, a recent Information Security Forum (2014) survey noted that "around 85% of Member organizations reported that their people were either unaware, or were aware but not taking all the correct actions to minimize [security] risk." Moreover, "75% of ISF Members have an ongoing awareness program, yet only 15% reported that they had reached that heightened level of awareness and positive behaviors that they are striving for."

These concerns are shared by others in related areas, such as crime science and organizational security: How do we persuade workers to follow simple, fundamental processes to protect themselves and others? These issues are raised in

***Corresponding author: Shari Lawrence Pfleeger,** Pfleeger Consulting Group, 4519 Davenport St NW, Washington, District of Columbia 20016, USA, Phone: +202 244 3740, e-mail: shari@pfleeger.com
M. Angela Sasse: Computer Science, University College London, London, UK
Adrian Furnham: Psychology, University College London, London, UK

other contexts, especially by behavioral scientists, to encourage worker, passenger and patient compliance. In this paper, we have reviewed what economists, sociologists and psychologists have discovered about effective behavior change, to identify factors leading to success. Each of the identified factors is underpinned by empirical evidence reported in solid, peer-reviewed studies. From these results, we have drawn together insights – well-known and well-accepted in their own disciplines – and derived from them a framework for understanding how organizations can successfully change security behavior in the long term. This new approach to understanding and improving security behavior is thought-provoking and leverages empirically-demonstrated long-term success in similar situations. To that end, we explore studies in these similar areas, summarize relevant findings, and integrate them into suggestions for building on existing work and transforming staff security behavior online.

2 Building on *Homo Economicus* and Swiss Cheese

Organizational leaders do or should care about security: The Ponemon Institute's Cost of Data Breach Study indicates that 35% of breaches are caused by human factors. (http://www.ponemon.org/library/2013-cost-of-data-breach-global-analysis⁻) To encourage secure behavior when using applications and communications technology, most invest in training to ensure their staff knows both security policies and how to use security tools. For staff, however, functionality usually trumps security: users circumvent security in order to focus on meeting deadlines, making tasks easier, and speeding interaction with colleagues.

To address this problem, some researchers have looked beyond technology for assistance. Initially, cyber security's technological genesis and effectiveness were viewed through an economic lens; accelerated by over a dozen Workshops on the Economics of Information Security (http://weis2014.econinfosec.org/past.php), concepts from traditional and behavioral economics have been applied to cyber security to help us understand the motivations for security- and privacy-based actions that seem otherwise to be counter-intuitive or even counter-productive. For example, Acquisti and Grossklags (2003) sought to understand how market behavior might influence security attitudes and behaviors. Herley (2009) noted that most users ignore security advice, because there is no economic incentive to do so. "Users' rejection of the security advice they receive is entirely rational from an economic perspective. The advice offers to shield them from the direct costs of attacks, but burdens them with far greater indirect costs in the form of effort."

Pfleeger and Caputo (2012) identified several areas of behavioral science beyond economics that could be useful not only in addressing our understanding

of user behavior but also in informing our design so that systems encourage good security behavior. Herzberg (1987) emphasizes that it is not enough to ask users to be careful: "What is the simplest, surest, and most direct way of getting someone to do something? Ask? But if the person responds that he or she does not want to do it, then that calls for psychological consultation to determine the reason for such obstinacy."

We know that once-a-year security reminders have limited effectiveness, but "improved" training seems to make little difference in employees' attitudes and reactions. Technologists tend to want to prescribe and proscribe: devise approved processes to keep organizations safe and secure. Indeed, employees who do not comply with policies are blamed as being the "weakest link" in the security chain. However, the safety literature suggests that such constraints and admonitions alone do not work.

Reason (2008), who has long studied safety and security habits and behaviors, found that if an organization views the "human as hazard" and prescribes only one way to do things, adherence and compliance often backfire. Reason points out that some accidents are inevitable. Layers of defense are like layers of Swiss cheese which, if aligned in the right way, will allow the enablers of bad outcomes to make their way through the holes. He notes in a variety of examples that "heroic actions" have prevented accidents from leading to even worse consequences. Yet heroic behavior does not just happen; organizations must invest in an environment that enables the heroic acts to occur. To create such an environment, Reason says the solution lies in emphasizing individual and collective "mindfulness": awareness of what might go wrong, and understanding of actions that could mitigate those effects. Weick and Sutcliffe (2001) explain that mindfulness is an attitude into which is woven preoccupation with failure, reluctance to simplify interpretations, sensitivity to operations, commitment to resilience and deference to expertise.

In essence, this approach uses a psychological rather than a technical solution to the problem. It advocates understanding the issue and problems from a user's perspective and then determining how messages about behavioral change can be most effective.

Thus, the essential question for technologists is: how do we encourage such mindfulness, so that employees become "security heroes" and advocates and who can recognize enabling vulnerabilities and take actions to plug them? The answers appear to lie in applying behavioral science: the broader set of factors that affect security behavior in practice. Security improvements may result from applying basic human factors knowledge (see sidebar) when we design, develop, use and maintain systems with a security component. But we currently lack similar guidance on using appropriate training, cues, rewards and motivation to create and nourish a healthy security culture.

Herzberg's work provides one of the keys to establishing this culture: understanding the difference between motivation and hygiene. He notes that "environmental factors (hygiene) can at best create no dissatisfaction on the job, and their absence creates dissatisfaction. In contrast, what makes people happy on the job and motivates them are the job content factors (motivators)." Thus, the key to enabling good security behavior may be providing good motivators. In turn, to motivate people appropriately, we must understand what they value and why.

Sidebar: Human Factors and Security

Human Factors techniques can maximize human performance while ensuring safety and security. Their key principle is designing technology that fits a person's physical and mental abilities: fitting the task to the human. Rarely should we fit the human to the task, because it requires significant organizational investment in training which, even when effective, still diverts time and effort away from critical activities. For example, an organization could train its employees to become memory artists, enabling them to juggle a large and changing number of PINs and passwords. Employees would then need most of their time for routines and exercises that reinforce memory and recall. That is, in addition to the time spent on the training course, employees still would have to spend time every day on memorizing and recalling passwords. It is more efficient to instead change security policies and implement mechanisms that enabling employees to cope without training. This approach is clear to behavioral experts but not always to those technologists and policy-makers who make and dictate security policies. But there is reported evidence of success in some areas. For example, the introduction of a low-effort, two-factor authentication solution (e.g. installing a token on the user's device, combined with a simple, memorable password) can improve security and reduce user workload. As a result, many organizations have now changed their password expiry policies, allowing users to keep passwords for longer periods of time, since there is evidence that compromised passwords tend to be exploited immediately and once. (http://www.schneier.com/blog/archives/2010/11/changing_passwo.html)

One key to understanding this approach is the ability to distinguish between production (*primary*) and enabling (*secondary*) tasks. Secondary tasks, such as safety and security-related behaviors, are not necessary for completing the production task. Rather, they are an investment to protect both individual and organization from harm: the enabling environment encouraged by Reason. Because human behavior is generally goal-driven, people use technology to get their jobs done. So a security task's time and workload should be as low as possible.

Humans are tempted to bypass secondary tasks, especially with primary task-related time or performance pressures. There are many examples of incentives that backfire, encouraging worse security behavior instead of better. For example, Sasse et al. (2001) describe an employee reprimanded by her line manager for not completing a production task on time; she forgot her password and could not access the necessary files. That employee will most likely write her passwords down to avoid being reprimanded again!

Security tasks often interrupt production tasks at critical points; resumption can require backtracking or repetition. This "restart cost" can be significant. Even seemingly less-disruptive security tasks such as warnings are rarely effective, because people see them as obstacles rather than protection. Wogalter and Feng (2010), using a *human-in-the-loop model*, show how applying human factors knowledge can minimize disruptions and maximize compliance.

One obvious way to ensure effective security behavior is to encourage habits that are skill-based rather than knowledge-based; the latter are slow and effortful, increasing workload. Psychologists Reason (2008), Haidt (2012), and Kahneman (2011) arrived at the same conclusion from slightly different perspectives: good habits must be integrated into business processes.

Thus, the best way to achieve compliance with security policies is to integrate security tasks with production tasks. Usability principles, such as exploiting the *modality of interaction,* can be applied. For instance, a production task involving typing might recognize the user from keystrokes, location and device, verifying user identity without disruption.

The physical and social context in which humans perform their tasks can also interfere with their security compliance. For instance, entering a regularly-used long passphrase on a keyboard may be low-effort, but entering it on a small device with a soft keyboard when standing on a crowded platform on a winter's day will take significantly longer. Social context matters, too: employees in shared offices may not want to divulge knowledge-based credentials when they can be overheard. Similarly, deploying screen-locks when leaving a computer may signal a lack of trust to colleagues.

In these ways, organizations that want to improve their security should apply human factors knowledge first. This self-evident first step is too often ignored.

3 From One to Many

Can an individual's demography, personality and values explain security choices? The answer to this question can suggest which approaches are likely to be most effective in encouraging good security behavior. Just as some people tend to be more "accident prone," some individuals may simply be more security conscious and compliant than others. It is important to know whether unsafe or insecure actions online are related to generally unhealthy traits.

For example, some researchers are investigating whether characteristics like paranoia, obsessive-compulsiveness, anti-social behavior or impulsiveness might predict unwelcome actions online. For instance, one recent study by McBride et al. (2012) correlated certain kinds of personality traits with likely cybersecurity behavior. They found that an "open" individual is less likely to obey a security protocol, but that an "open" person with a low sense of self-efficacy is more likely to obey it. Empirical work in this area is in its infancy but could yield some important information about how to target different groups in different settings with relevant information that will encourage good practice.

There are also important sociological implications for security science. Durkheim (1897) wrote that, "Man cannot become attached to higher aims and submit to a rule if he sees nothing above him to which he belongs." Haidt (2012) emphasizes that:

> "Utilitarians since Jeremy Bentham have focused intently on individuals. They try to improve the welfare of society by giving individuals what they want. But a Durkheimian version of utilitarianism would recognize that human flourishing requires social order and embeddedness. ... social order is extraordinarily difficult to achieve. ... binding foundations – Loyalty, Authority and Sanctity – have a crucial role to play in a good society."

In other words, security issues are embedded in, and deeply influenced by, social context such as corporate and national culture. In this sense, these issues have to be understood and addressed before any successful intervention program can be successfully introduced.

4 The Effort of Security

Recognizing the security burden is important. Muraven et al. (2008) demonstrated that tasks related to compliance require us to tap a limited amount of "vitality" needed for self-control; using a lot of self-control in one activity leaves little for later, more important activities. Kahneman (2011) illustrates (in Figure 1) the steps we might take to provide "cognitive ease" and reduce the "cognitive load."

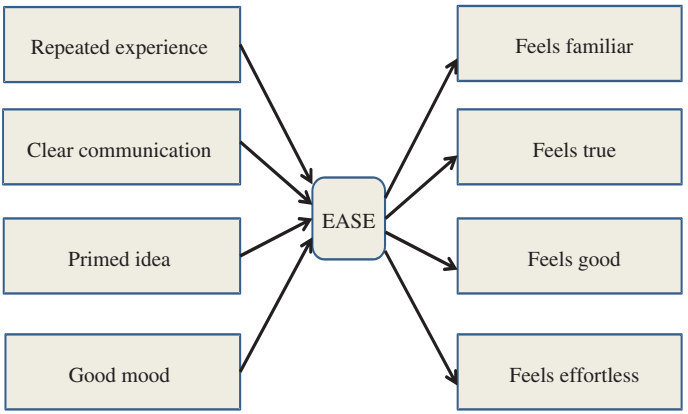

Figure 1 Causes and Consequences of Cognitive Ease (adapted from Kahneman 2011).

It is not by chance that the concept of ease is used a great deal in advertising. Indeed, branding a service or product as "easy" conveys an important message to consumers: Easy-Off oven cleaner, EasyJet Airlines, Easy-PC, and Easy-Flo Central Vacuum Cleaners are just a few examples where branding stresses minimal difficulty or discomfort. Behavioral economists explore how we can design human systems that make life easier for the user and that therefore should ensure greater compliance. Some of their ideas, such as priming people with security words and images, are already being used, and the ideas' effectiveness is being tested.

For example, Beautement et al. (2008) describe the energy required to comply with security procedures. Employees, not necessarily lazy or selfish, are prepared to expend a reasonable amount of effort, called a *compliance budget*, to keep the organization safe. Human factors knowledge (both common sense and personal experience) tells us that users are tempted to shortcut secondary tasks requiring high workload. The compliance budget is a user's way of keeping a mental tally of that effort. The effects on the compliance budget are cumulative, so that even a succession of reasonable-effort security tasks leads to short-cutting.

The lesson here is that, to encourage employee compliance with security policies, organizations should ensure that the daily security workload is manageable on individual tasks and overall. Both the number of security tasks and each task's effort should not drain the energy reservoir unnecessarily.

So how, as technologists, policy-makers and researchers, can we continue to address this goal? The remainder of our article provides a framework and guidelines based on solid empirical, behavioral-science-related findings.

We begin by examining the meaning of organizational culture and its role in creating an environment for positive security habits. We then show how Haidt's

(2012) moral foundations theory can be applied to help us understand both individual and group security actions. Next, we develop a taxonomy of security-related values that can be used to tailor security training, messages and even system design to encourage "good security hygiene." But good hygiene (necessary but not sufficient for a security culture) involves developing good security habits (for individuals) and good security routines (for organizations). We review the empirical behavioral science literature about habit formation and modification and apply it to security issues. With these foundations, we build a multidimensional framework for understanding how individuals and groups perceive security that can drive new ways to build and use systems. Finally, we pose a host of open research questions whose answers can enable organizations to create and nourish a security culture.

5 Enhancing Security Culture

Managers often talk about creating or improving their security culture, and they even discuss culture as a "security tool." (See, for example, http://issuu.com/pippinkellic/docs/human_behavior_overview_u.s.) But what does that mean, and how do we use culture to improve security behavior?

Generally, "culture" refers to a group's set of shared beliefs and values, reflected in the organizational practices. Schein (2004) explains that there are three levels of an organization's culture: artifacts and behaviors, espoused values, and underlying assumptions. Each level is evident to an outside observer. For example, artifacts are tangible, overt and identifiable, and they can include office furniture, dress codes, and even office jokes. Espoused values include not only stated values but also public enforcement (such as punishment for discriminatory acts). Underlying assumptions are shared actions and attitudes that are woven into everyday office activities.

There are many different conceptions of corporate and national culture, some offering a dimensional and others a categorical approach. For example, Schein (1996) explains how an organization's culture relates to eight "anchors" of an individual's career: autonomy and independence, security and stability, technical-functional competence, general managerial competence, entrepreneurial creativity, service or dedication to a cause, pure challenge, and life style. Even when defined quite simply as "the way we do things around here," culture is recognized as a powerful force in ensuring compliance Thus, many culture change interventions first set out to establish and define the organizational or departmental culture and then to implement a series of very specific processes to bring about change.

Organizational change is a long-term and costly business, only sometimes characterized by success (Furnham 2005). So additional insight is needed for improving the likelihood of positive change. The cultural dimensions by themselves do not suggest strategies for understanding and improving security culture. However, their underlying morals and values may hold the key to improved security (and other) practices, because values can impel individuals to adopt good security habits.

6 Moral Foundations and Security Values

Values are the beliefs in which people have an emotional investment. As basic convictions on how to conduct yourself in society, they guide you in living your life in a personally or socially preferable way. That is, values tell you how to live life "properly," according to your value system. Values are important because they

- Provide understanding of attitudes, motivation and behaviors
- Influence our perception of the world around us
- Represent interpretations of "right" and "wrong"
- Imply that some behaviors or outcomes are preferred over others

Morals involve the values that distinguish right from wrong, so they govern behaviors, priorities and choices. "Moral systems are interlocking sets of values, virtues, norms, practices, identities, institutions, technologies, and evolved psychological mechanisms that work together to suppress or regulate self-interest and make cooperative societies possible." (Haidt 2012). Haidt's extensive empirical validation of moral systems' influence political actions means that moral systems can influence security-related choices, too.

Many people assume that morality can be explained using only one criterion: *primum no nocere* (first, do no harm). Indeed, people who think that their actions are harming neither organizational nor employee security feel as though they are acting correctly. But that is not always the case: What is fine for one person may be considered harm by another whose moral system is different.

To see why, consider how moral systems differ. Haidt's empirical research suggests that, no matter how morals are developed, they are multi-faceted, guide an individual's choices and behaviors, and can be expressed in terms of the six dimensions shown in Table 1. For example, the care-harm dimension does not explain why some people are disgusted by website defacement, while others are ambivalent. But the sanctity-degradation dimension explains it; it reflects

Table 1 Six Dimensions of Moral Foundations.

Dimension of Moral Foundation	Meaning	Characteristic Emotions	Related Virtues
Care vs. Harm	Being sensitive to signs of suffering and need; dislike of cruelty	Compassion	Caring, kindness
Fairness vs. Cheating	Reaping the rewards of collaboration without being exploited	Anger, gratitude, guilt	Fairness, justice, trustworthiness
Liberty vs. Oppression	Being sensitive to controlling behavior	Freedom, restraint, resistance, reactance	Openness
Loyalty vs. Betrayal	Forming and maintaining coalitions	Group pride, rage at traitors, trust	Loyalty, patriotism, self-sacrifice
Authority vs. Subversion	Forging relationships that will benefit us within social hierarchies	Respect, fear	Obedience, deference
Sanctity vs. Degradation	Being sensitive to an array of symbolic objects and threats; investing objects with value (positive and negative) beyond their usual meaning	Disgust, reverence	Temperance, chastity, piety, cleanliness

Adapted from Haidt 2012.

the way some people invest an item with meaning beyond its usual value. The website is a symbol of the organization whose information it conveys, so disrespect for the website equates to disrespect for the organization. Taken together, these dimensions and their associated emotions and virtues can explain how an individual perceives an item or action, and how he or she reacts to it.

This validated framework (as described in Haidt 2012) tells us that if we know the moral profiles for individuals and groups, we can see where they stand on these various dimensions, and how that standing relates to a positive security culture.

Moreover, the moral foundations often lead to strong reactions to situations – strength that can be leveraged to find ways to influence security-related behaviors. We have examined each of the six dimensions, to see what each implies for security.

Listed again in Table 2, each moral dimension is associated with security challenges, triggers and actions. For example, as we have seen, the sanctity-degradation foundation suggests that organizational symbols such as websites, flags and logos may be invested with meaning. To encourage a security culture, the organization can react by putting in place protections for its website, as well as a reporting scheme for notifying the organization if defacement takes place.

By assessing these dimensions, triggers and actions, an organization interested in improving security culture can see where security help is needed, and then put in place awareness mechanisms (e.g. warnings, informational

Table 2 Moral Foundations' Implications for Security Challenges, Triggers and Actions.

Dimension of Moral Foundation	Security Challenges	Security Triggers	Security Actions
Care vs. Harm	Protect and care for organizational assets	Assets labeled clearly with their value to the organization and the individual	– Awareness about assets and their value – Provide effective training and education about good security practices
Fairness vs. Cheating	Reap benefits of organizational membership	Practices that can affect other people's security and well-being	– Awareness of possible harm to other people – Awareness of harm to organization
Liberty vs. Oppression	Freedom to act but within organizational policies and constraints	Reminders about security policies and procedures	– Effective communication and enforcement of security policies and procedures – Integration of policies and procedures into business practices
Loyalty vs. Betrayal	Form cohesive coalitions around effective leaders to further personal and organizational goals	Information about security practices of others in same or similar groups	– Information about similar practices (e.g. "87% of employees did not click on this link")
Authority vs. Subversion	Forge beneficial relationships within hierarchies	Reminders about access controls and policies	– Integration of access warnings and messages
Sanctity vs. Degradation	Avoid degradation of organizational symbols and policies	Symbols representing the organizational brand, such as web sites, flags, logos; policies specifying that, when not enforced, have significant consequences	– Protection of symbols from defacement – Reporting procedures for detection of symbol defacement – Serious consequences for contravening policy

websites, reminders) and training schemes that appeal to each employee's moral values. These mechanisms and schemes can reflect an organization's culture as well as an individual's preferences. By approaching mechanisms, awareness and training in this way, an organization can take advantage of each employee's predispositions to perceive and react; the resulting outcomes should feel more natural to the employee and be consonant with the employee's other behaviors.

7 Changing Security Habits

The long-term goal is to improve each employee's security habits, making his or her security actions natural – thereby not depleting each person's compliance budget. Although we like to think that our choices are made based on reasoning rooted in our values, Haidt (2012) summarizes research that clearly shows that intuitions come first, then strategic reasoning second. Thus, a key to changing security habits may be changing intuitions based on individual and group moral values, so that people instinctively believe that the new ways will work better than the old ways.

How do we change these intuitions? By changing our habits. Much of our day involves habits rather than conscious decisions. We awaken, make breakfast, and travel to work by relying on a set of learned behaviors, each of which is triggered by a cue of which we may not even be aware. Andrews (1908) describes a habit as a "fixed way of thinking, willing or feeling acquired through previous repetition of a mental experience." Duhigg (2012) refines the notion by calling it a certain behavior that occurs in response to a certain cue that in turn leads to a certain reward. Our workplace behaviors (e.g. submitting time sheets, taking a lunch break, attending staff meetings) often become habits, sometimes prompted by a set of routines encouraged by our organizations.

Much recent psychological research has attempted to understand when and why we experience quick, lazy, intuitive, heuristic and habitual thinking that is prone to error. To explain the causes, Stanovich and West (2000) distinguish between System 1 (what Reason called skill-based) and System 2 (what Reason calls knowledge-based). System 1 "has learned associations between ideas ... and learned skills such as reading and understanding nuances of social situations." By contrast, "the highly diverse operations of System 2 have one feature in common: they require attention and are disrupted when attention is drawn away. ... Among the basic features of System 1 is its ability to set expectations and to be surprised when these expectations are violated. ... System 2 can reset the expectations of System 1 on the fly." (Kahneman 2011). Haidt (2008) calls System 1 our emotional self and System 2 our rational self, using the metaphor of a small rider (System 2) astride a large elephant (System 1) to convey the difficulty our rational minds face when trying to control our instincts and emotions.

Habits help to address this difference, using automatic action to accustom System 1 to follow System 2's instructions. Heath and Heath (2010) explain that habits make us efficient: "the elephant gets things done." But automatic behavior also means that individuals tend to choose short-term gratification over longer-term achievements: they want to get the reward as quickly as possible. "Changes often fail because the rider simply cannot keep the elephant on the road long enough to reach the destination." (Heath and Heath 2010).

In the security context, organizations may choose to invest in security to assure their long-term survival, but individuals will be inclined to instead focus on the rewards of completing their primary task (and perhaps take security shortcuts to preserve their compliance budget).

Once established, behavioral and cognitive habits are very hard to change. Maio and his colleagues (2007) point out that many behaviors change very slowly, if at all. Moreover, it is not enough to change attitude; attitudinal change does not always end with behavioral change. For example, Hobson (2003) found that changed attitude toward climate change did not alter habits affecting climate change. Kempton et al. (1992) demonstrated that one-time change in behavior is relatively easy, compared with long-term, repetitive behavioral change.

Paradoxically, security systems have conditioned many individuals to respond to security cues by ignoring or bypassing them whenever possible. That is, the security systems have encouraged bad, rather than good, security habits. As an example, consider security warnings: most individuals have been conditioned to understand that there are few or no consequences to ignoring warnings about possible insecure files, certificates or sites; as a result, they have developed a habit of deleting or ignoring the system's warnings boxes. In a recent empirical study, Krol et al. (2012) found that 81.7% of their study participants ignored warnings before downloading a file onto their own computer. In the debrief interview, most participants said that they had ignored warnings before, "and since nothing bad happened," went ahead with their intended action anyway. In other words, participants assumed that no harm was done: nothing bad had happened, and the users were seemingly unaware that if they had downloaded a piece of malware, the consequences might not have been immediately obvious. This result was confirmed in the McBride et al. study; low likelihood of punishment led to higher likelihoods of undesirable security behaviors. Thus, a security warning without consequences has become a cue that triggers a habit of dismissing it and getting on with the primary task: the reward. Moreover, every time this happens, the habit is reinforced.

Even when there are consequences, it matters whether the bad behavior affects the individual or someone else. For example, Grant and Hofmann (2011) found that health care professionals are more likely to wash their hands when reminded of the consequences for others than when reminded of the consequences for themselves.

So how can we break this habit cycle? Security awareness and training activities are often cited as ways of breaking the cycle and establishing better habits. Egelman et al. (2008) reported that active rather than passive warnings, incorporating explanations of threats and consequences, stopped four of five participants from succumbing to a spear phishing attack. But in the organizational context,

Caputo and her colleagues (2014) found that warnings making employees aware of spear phishing attempts and educating them about prevention strategies had no effect because the employees were not reading the warnings. Indeed, some of the study subjects ignored the warnings, thinking they were themselves evidence of malware! So awareness and training must be approached differently if organizations are to develop an effective security culture.

Organizations can use knowledge about habit formation to improve their employees' security behavior. Duhigg (2012) suggests that an individual's behavior can be changed by inserting a *new routine* between cue and reward. In security, this strategy means replacing the insecure behavior with a secure one: the goal of security awareness and training. Yet this strategy fails if the reward is not consistent with the action. The goal is primary task completion, but the inconsistent security action can actually postpone goal attainment – and with little or no discernible benefit. In such situations, we need solutions more aligned with the goal. Ideally, we should make the secondary security task disappear, and instead assist individuals in completing their primary task.

Several attempts have been made to eliminate security tasks. For instance, consider the threat of illegitimate product sites online. For many popular products, as many as seven out of the top ten listed search results offer fake products or are phishing for personal details (Edelman and Rosenbaum 2006). In response to this problem, First Cyber Security has developed a modified search engine, called Safe Shop Window, (http://www.safeshopwindow.co.uk/?att=fcs), that shows only legitimate retail sites when customers search for a product. This solution removes the traditional security steps: producing a warning for suspected illegitimate sites and possibly restricting the searcher's behavior in some way.

Many other security problems could more effectively and efficiently be solved by integrating security with primary tasks, thereby removing the disincentive of increased workload: what Beautement et al. (2008) called *friction*. Such strategies would also change the user's general perception of security as an effort drain, making security align with one or more of the six moral dimensions.

To achieve this alignment, system designers (who, as Herley (2009) notes, "value users' time at zero") could switch their focus from changing users' security habits to designing security that at least fits into primary tasks or at most requires a minimal amount of extra effort. In other words, we should examine ways to improve designers' habits as well as users' security habits; the former can enable the latter.

Effective habit change, no matter the target audience, requires more than an understanding of Systems 1 and 2 and of cue, behavior and reward. Kahneman (2011) notes that, "System 1 continuously generates suggestions for System 2: impressions, intuitions, intentions, and feelings. If endorsed by System 2,

impressions and intuitions turn into beliefs, and impulses turn into voluntary actions." Heath and Heath (2010) use this characterization to identify three requirements for effective habit change: applying System 2's careful analysis, endorsing System 1's instincts, and shaping the path toward habit change.

8 Applying System 2's Analysis

To apply System 2, the organization or the system must provide clear instructions about what to do and what goals will be achieved. If people fail to change habits, it is usually because of:

- Ambiguity: They cannot figure out what they should be doing.
- Vagueness: The targets are vague.
- Overload: They are trying to change too much at the same time.

Kirlappos and Sasse (2012) diagnosed all three mistakes in the security awareness and education campaigns they examined. Security awareness needs to have concrete goals for each habit, be designed as an ongoing effort, and tackle one change at the time. For example, security awareness might start with an easily-achievable goal that encourages employees to feel successful about their security behavior:

- Goal: Zero unencrypted USB devices by the beginning of next month
- Monitor Change Over Time: Evaluate USB devices each month, give feedback to show adopters their progress, and tell laggards what is needed for making progress
- Target: One device type

In addition, habit change activities should acknowledge that people tend to make changes to habits that are easier to modify but may not have as much impact. (Kempton et al. 1985; Diekmann and Preisendörfer 1992). Indeed, once a "token modification" is made, users feel as if they have contributed to the security effort and need not do more.

9 Endorsing System 1's Instincts

To motivate individuals to change, security awareness must address their emotive side, evoking a visceral response that confronts individuals with the extent of the problem or the benefits. To see why, consider how people who develop bad habits

can be motivated to change them. For example, over-eaters, presented with a catalogue of food they habitually eat in a month or the life expectancy associated with their weight, often change their habits. Security motivation can similarly jolt individuals out of comfortable beliefs. Symantec's Race to Stay Safe tests your ability to distinguish a bona fide from a corrupt website: https://www.staysecureonline.com/staying-safe-online. It shows ten examples of two near-identical websites; the corrupt one has at least one characteristic that should make you suspicious. When people choose the wrong one, they are more receptive to being told about features they should check before using a website. Habit change might also be motivated by showing interviews with victims of identity theft, or displaying bundles of $50 notes to visualize the cost of cleaning infected machines.

10 Shaping the Path to Habit Change

Since changing habits is difficult, it is important to remove obstacles on the path to establishing the new habit. Obstacles can distract individuals from the goals, or provide excuses to slip back into the old habits. When security is unusable and cumbersome, reversion to the old, more efficient shortcut is pre-programmed. More importantly, organizations can be proactive, designing practices and tools to assist people in changing their habits.

Hodgson (2004) noted that "Routines are the organizational analogues of habits." Heath and Heath (2010) argue that their three principles apply to organizational change: "if you reach the riders in your team but not the elephants, team members will have understanding without motivation. If you reach the elephants but not the riders, they'll have passion without direction."

Organizations can appeal to employees' rational side to follow security rules, but when workers face many demands, they find it hard to motivate themselves; change is difficult because people wear themselves out. If organizations try to force changing without motivating and smoothing the path, both they and their employees will run out of resources without accomplishing the goal. Thus, to make extensive changes, an organization must focus on *keystone habits*: habits that "start a process that, over time, transforms everything." Keystone habits work because "habits have the power to start a chain reaction, changing other habits as they move through the organization." (Duhigg 2012).

There are many examples of successful habit change using this principle. For instance, O'Neill turned around Alcoa, an ailing company, by making safety a keystone habit (Cable 2013). When he became CEO, O'Neill stunned colleagues and investors by making safety his top priority. He picked safety because it was a goal the affected the whole company, and with which no one could disagree.

He set a concrete goal: zero accidents. By changing how the company handled safety, he created "a habit of excellence ... an indicator that we are making progressing changing our habits across the entire institution."(Duhigg 2012). Safety provided the focus for discussion and collaboration throughout the organization to achieve the one goal, which in turn started to shift, dislodge and remake other patterns. Keystone habits work because "success does not depend on getting every single thing right, but instead identifying a few priorities and fashioning them into powerful levers."

What keystone habits can be used to instill a security culture? "Good leaders seize crises to remake organizational habits" and routines (Duhigg 2012). So security breaches can draw attention to policies and practices that can spawn transformation; employees may pay attention to changes during a crisis that might meet resistance in more comfortable times.

11 Using Moral Foundations to Motivate Security Awareness and Action

Researchers such as Bandura (2007) and Blankenship and Wegener (2008) have used values as a context for habit change, especially in addressing climate change. In the same way, we can build a multi-dimensional framework for understanding how individuals and groups perceive security that can drive new ways to build and use systems. Our framework uses the six dimensions of Haidt 2012's research on moral foundation, examining them from the perspective of habit formation. For each dimension, we look for a keystone habit that reflects that dimension and can be used to apply System 2's analysis, endorse System 1's instincts, and shape the path.

Heath and Heath (2010) explain how to accomplish these steps. To effectively influence System 2, we appeal to a person's rational side using three strategies:

- *Find the bright spots*: Look for strategies that are already working and repeat them in ways that encourage employees to meet the organization's goal.
- *Script the critical moves:* Break the practices into bite-sized pieces, so that people understand exactly how to get from here to there.
- *Point to the destination*. Show people what the goal looks like and give them signals about how much progress they are making.

To trigger System 1's instincts, we appeal to a person's emotional side:

- *Identify the instinct or feeling*: Make the results visceral, connecting the desired outcome to something that the employees know and understand.

Table 3 Moral Foundations and Habit Formation to Build Security Culture.

Dimension of Moral Foundation	Keystone Habits	Apply System 2's Analysis	Endorse System 1's Instincts	Shape the Path
Care vs. Harm	Responsibility for all assets and risks assigned	– Assets labeled with their value to the organization and the individual – Clear consequences for irresponsible behavior, whether or not it leads to security problem	– Show how secure we are – Provide relevant training updates to responsible parties	– Use safer tools – Showcase and celebrate behavior – Show how to avoid risky behavior
Fairness vs. Cheating	Reward good security behavior that protects everyone	– Communicate benefits of compliance. – Provide examples of consequences (damages) resulting from non-compliance	– Associate positive feelings/images with "doing the right thing"	– Provide checklists
Liberty vs. Oppression	Consonant with organizational culture, develop consensus on security policies and procedures	– Provide reminders about security policies and procedures	– Build group trust – Remind employees that they are valued and trusted	– Before transgressions occur, show all alternative but correct actions
Loyalty vs. Betrayal	Form cohesive coalitions to monitor security health	– Show how risk-taking/shortcuts might affect colleagues, customers, the organization	– Associate shortcuts with negative traits	– Provide accessible help/guidance for anyone not sure what the right choice is
Authority vs. Subversion	Establish clear security rules and responsibilities	– Make clear that organization has made careful choices about security, and has expertise	– Make clear that subversion is not heroic, but parasitic behavior that damages colleagues' good work. Senior staff could lead by example, as role models, so that staff could follow leaders' behavior	– Make sure rules are visible, easy to understand, easy to comply
Sanctity vs. Degradation	Provide labels to make clear what assets are most valuable	– Provide asset inventories – Remind users of asset value with color-coding or other signs	– Advertise key transgressions	– Provide concrete "how to" examples of applying the values

- *Shrink the change*: When the full set of changes is daunting, break the change into pieces that are easy to accomplish.
- *Grow the people*: Cultivate a mindset that marries the people to their goal and gives them an identity to which they aspire.

Finally, to shape the path, we can alter the environment, build habits and rally the team. Sometimes, the environment itself acts as a barrier to change. By changing the environment (e.g. by using a safer search engine), we make it easier for employees to develop the desirable habits. When there are aspects of the desirable habits that can be organized so that they do not deplete the compliance budget, we can invoke those changes: use checklists, reminders and warnings, for example. And when the desired habits have been instilled in some employees, we rally the team by advertising those successes to the other employees.

Table 3 displays the combination of moral foundations theory with habit formation.

12 Conclusions, Open Research Questions and Next Steps

In previous sections, we presented a framework based on empirical validation of both moral foundations theory and habit formation that can be used to set us on the path toward a more robust security culture. We have also shown linkages between problems solved this way in other domains with problems we experience in security; the linkages suggest likely success in developing a security culture. In this section, we examine in more depth the short- and long-term activities in which we can engage.

As noted earlier, the most desirable situation is making security behavior seamless: browsers that automatically screen out suspect web sites, tools that control access to valuable data, and more. There is no way to make all choices for a user, so the choices must be infrequent and require only minimal distraction from primary tasks. Thus, in the short term, we can focus on several key activities, each with an accompanying research question:

- *Design systems so that security decisions are spread out, not clustered together to deplete a user's compliance budget*. Research question: By how much does each security action deplete a user's energy?
- *Design systems to provide reminders of good security choices*. Research question: How often is too often? How infrequently renders the reminder system ineffective?

– *Assess each individual's place in the six-dimensional value space, and tailor training and messages to the result.* Research question: Survey instruments exist to assess each dimension. How can they be tailored to focus on security aspects of each dimension?

In the long-term, more difficult questions should be addressed.

– How do we separate personal from professional security behavior and culture?
– How does each behavior relate to the value dimensions? That is, rewards, warnings, and trust relationships can be mapped to the six dimensions. Then, habit formation can be based on the six-tuple, so that all aspects of a behavior are considered.
– Can underlying values be changed from negative to positive? That is, are there people whose values suggest that appropriate security behavioral change would be difficult or even impossible? In such cases, is it possible to change the environment to suit the values, or must a user be prevented from performing certain jobs?
– Is there a risk that changed behavior will revert to old, undesirable habits over time? Inoculation theory (McGuire 1961) examines how attitudes and beliefs remain consistent despite attempts to persuade change. This area of inquiry may have useful application to cyber security.

The answers to these open research questions, provided by continuing hypothesis formulation and empirical investigation, will enable us to create and nourish a security culture. We have stressed the importance of a multi-disciplinary human factors focus, with empirical investigations that seek to understand how and why habits form and how they can be changed by a variety of interventions. The days of prescriptive technological solutions to security issues are surely over, given the data that suggest not only that they do not work but also that they frequently lead to the "law of unintended consequences" whereby they exacerbate security problems.

References

Acquisti, Alessandro and Jens Grossklags (2003) "Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior," *Proceedings of the Second Workshop on the Economics of Information Security*. May 2003.

Andrews, B. R. (1908) "Habit," American Journal of Psychology, 14(2):121–149.

Bandura, A. (2007) "Impeding Ecological Sustainability Through Selective Moral Disengagement," International Journal of Innovation and Sustainable Development, 2(1):8–35.

Beautement, Adam, M. Angela Sasse and Mike Wonham (2008) "The Compliance Budget: Managing Security Behavior in Organizations," *New Security Paradigms Workshop*. Available at: http://www.nspw.org/papers/2008/nspw2008-beautement.pdf.

Blankenship, K. L. and D. T. Wegener (2008) "Opening the Mind to Close It: Considering a Message in Light of Important Values Increases Message Processing and Later Resistance to Change," Journal of Personality and Social Psychology, 66:1034–1048.

Cable, Josh (2013): "NSC 2013: O'Neill Exemplifies Safety Leadership," *EHS Today*, 3 October 2013, Available at: http://ehstoday.com/safety/nsc-2013-oneill-exemplifies-safety-leadership.

Caputo, Deanna, Shari Lawrence Pfleeger, Jesse Freeman and M. Eric Johnson (2014) "Going Spear Phishing: Exploring Embedded Training and Awareness," IEEE Security & Privacy, 12(1):28–38.

Diekmann, A. and P. Preisendörfer (1992) "Personliches umweltverhalten: Diskrepanzen zwischen anspruch und wirklichkeit," Kölner Zeitschrift Für Soziologie Und Sozialpsychologie, 44:226–251.

Duhigg, Charles (2012) *The Power of Habit: Why We Do What We Do in Life and Business*. New York: Random House.

Durkheim, Emile (1897) *Le Suicide*, Alcan Press, Paris, 1897. (J. A. Spalding and G. Simpson trans.), New York: Free Press 1951.

Edelman, Ben and Hannah Rosenbaum (2006) "The Safety of Internet Search Engines," *MacAfee*, 12 May 2006, Available at: http://www.siteadvisor.com/studies/search_safety_may2006.html.

Egelman, Serge, Lorrie Faith Cranor and Jason Hong (2008) "You've Been Warned: An Empirical Study on the Effectiveness of Web Browser Phishing Warnings," *Proceedings of Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. Available at: http://www.guanotronic.com/ serge/papers/warned.pdf.

Furnham, Adrian (2005) *The Psychology of Behaviour at Work: The Individual in the Organization*. Hove: Psychology Press.

Grant, Adam and David Hofmann (2011) "It's Not All About Me: Motivating Hospital Hand Hygiene by Focusing on Patients," Psychological Science, 22:1494–1499.

Haidt, Jonathan (2012) *The Righteous Mind: Why Good People Are Divided by Politics and Religion*. New York: Pantheon Books.

Heath, Chip and Dan Heath (2010) *Switch: How to Change Things When Change is Hard*. New York: Broadway Books.

Herley, Cormac (2009) "So Long, and No Thanks for the Externalities: The Rational Rejection of Security Advice by Users," *Proceedings of the New Security Paradigms Workshop*. Available at: http://research.microsoft.com/en-us/um/people/cormac/papers/2009/SoLongAndNoThanks.pdf.

Herzberg, Frederick (1987): "One More Time: How Do You Motivate Employees?" Harvard Business Review 65(6):109–120.

Hobson, Kersty (2003): "Thinking Habits into Action: The Role of Knowledge and Process in Questioning Household Consumption Practices," Local Environment, 8(1):95–112.

Hodgson, Geoffrey M. (2004): "The Nature and Replication of Routines," Available at: http://www.gredeg.cnrs.fr/routines/workshop/papers/Hodgson.pdf.

Information Security Forum. (2014) "From Promoting Awareness to Embedding Behaviours," Available at: https://www.securityforum.org/shop/p-71-170.

Kahneman, Daniel (2011) *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux.

Kempton, W., C. K. Harris, J. G. Keith and J. S. Weihl (1985) "Do Consumers Know What Works in Energy Conservation?" Marriage and Family Review, 9:115–133.
Kempton, W., J. M. Darley and P. C. Stern (1992) "Psychological Research for The New Energy Problems: Strategies and Opportunities," American Psychologist, 47(10):1213–1223.
Kirlappos, Iacovos and M. Angela Sasse (2012) "Security Education Against Phishing: A Modest Proposal for a Major Rethink," IEEE Security and Privacy, 10(2):24–32.
Krol, Kat, Matthew Moroz and M. Angela Sasse (2012) "Don't Work. Can't Work? Why It Is Time to Rethink Security Warnings," *Proceedings of CRISIS*.
Maio, G. R., B. Verplanken, A.S.R. Manstead, W. Stroebe, C.S. Abraham, C. S., P. Sheeran and M. Conner (2007) "Social Psychological Factors in Lifestyle Change and Their Relevance to Social Policy," *Social Issues and Policy Review*, 1:99–138.
McBride, Maranda, Lemuria Carter and Merrill Warkinten (2012) *Exploring the Role of Individual Employee Characteristics and Personality on Employee Compliance with Cyber Security Policies*. Technical Report, RTI International.
McGuire, W. J. (1961) "The Effectiveness of Supportive and Refutational Defenses in Immunizing Defenses," Sociometry, 24:184–197.
Muraven, Mark, Marylène Gagné and Heather Rosman (2008) "Helpful Self-Control: Autonomy Support, Vitality and Depletion," Journal of Experimental and Social Psychology, 44(3):573–585.
Pfleeger, Shari Lawrence and Deanna Caputo (2012) "Leveraging Behavioral Science to Mitigate Cyber Security Risk," Computers & Security, 31:597–611.
Reason, James T. (2008) *The Human Contribution: Unsafe Acts, Accidents and Heroic Recoveries*. Farnham, Surrey: Ashgate Publishing.
Sasse, M. Angela, Sacha Brostoff and Dirk Weirich (2001) "Transforming the 'Weakest Link': A Human/Computer Interaction Approach to Usable and Effective Security," BT Technology Journal, 19(3):122–131.
Schein, Edgar H. (1996) "Career Anchors Revisited: Implications for Career Development in the 21st Century," The Academy of Management Executive, 10(4):80–88.
Schein, Edgar H. (2004) *Organizational Culture and Leadership*. San Francisco: Jossey-Bass.
Stanovich, Keith E. and Richard F. West (2000) "Individual Differences in Reasoning: Implications for the Rationality Debate," Behavioral and Brain Science, 23(5):645–665.
Weick, Karl E. and Kathleen M. Sutcliffe (2001) *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Francisco: Jossey-Bass.
Wogalter, Michael S. and Eric Feng (2010) "Indirect warnings/instructions Produce Behavioral Compliance," Human Factors and Ergonomics in Manufacturing and Service Industries, 20:500–510.