Chapter 3
The "Human Factor" in Cybersecurity:
Exploring the Accidental Insider

Lee Hadlington
De Montfort University, UK

ABSTRACT

A great deal of research has been devoted to the exploration and categorization of threats posed from malicious attacks from current employees who are disgruntled with the organisation, or are motivated by financial gain. These so-called "insider threats" pose a growing menace to information security, but given the right mechanisms, they have the potential to be detected and caught. In contrast, human factors related to aspects of poor planning, lack of attention to detail, and ignorance are linked to the rise of the accidental or unintentional insider. In this instance there is no malicious intent and no prior planning for their "attack," but their actions can be equally as damaging and disruptive to the organisation. This chapter presents an exploration of fundamental human factors that could contribute to an individual becoming an unintentional threat. Furthermore, key frameworks for designing mitigations for such threats are also presented, alongside suggestions for future research in this area.

INTRODUCTION

The focus of this current chapter is to examine the impact human factors, including aspects of personality traits or cognitive factors that can serve to influence cybersecurity practices and behaviors. The background against which this exploration is framed is related to the insider threat, more specifically those that have no specific motive or malicious intent. The chapter will begin with an examination of key statistics related to cybercrime in business as well as introducing current concerns related to the 'insider threat'. The typology of the insider threat will be discussed in brief, but then will shift to focus more directly on the notion of an 'accidental insider' – those individuals who have no malicious intent to commit transgressions of cybersecurity, but do so through misjudgment, ignorance and lack of understanding/knowledge.

DOI: 10.4018/978-1-5225-4053-3.ch003

Following on from this, the focus will then turn towards research examining key human factors that could influence the cybersecurity posture of the individual. This includes potential links between psychology traits such as impulsivity, decision-making and conscientiousness and information security. The concluding aspects for the chapter will focus on key techniques and frameworks that have the potential to change the behaviors of end-users. These techniques hopefully move individuals towards better cyber-inoculation, and provide mitigation for the threat from the accidental insider.

BACKGROUND

In a recent report published by the Office of National Statistics (ONS, 2016) it was estimated that online fraud was costing companies an estimated £193bn. Furthermore, the survey also noted that 5.8 million individual incidents of cybercrime had been reported in the year 2015-16; these were split between fraudulent activities (bank/credit card account fraud/advance fee fraud) and computer misuse (distribution of computer viruses/unauthorized access to computers/hacking). The Business Crime Survey (BCS, 2015) also noted a 55% increase in reported online fraud between 2014-15. In the same report, one of the key concerns raised was the growing threat from individuals within the organization, or the so called 'insider threat'. This latter point is mirrored by an apparent realization by researchers within the information security community that, for the most part, the weakest element in the cybersecurity chain is that of the human (Anwar et al., 2016; Nurse, Creese, Goldsmith, & Lamberts, 2011; Sasse, Brostoff, & Weirich, 2001; Sasse & Flechais, 2005).

In the context of the continued fight to protect business and organizations from the threat being posed by information theft and cybercrime a great deal of attention is devoted to improving the existing security infrastructure (Pfleeger & Caputo, 2012). Attempts to enhance network security via technological solutions such firewalls, intrusion detection, and biometric devices provide some legitimate protection against a wide variety of threats. However, these steps make an assumption that all threats to the security of the organization are inward facing, and come from an external source or attacker. Early commentators in the area of cybersecurity noted that one of the biggest barriers to creating effective information security strategies is the human elements within the system (Whitten & Tygar, 1998). From a usability perspective it is noted that, for the most part, security protocols and systems are either too confusing or too difficult for the average end-user to engage in effectively (Whitten & Tygar, 1998; Sasse & Flechais, 2005). Accordingly, Sasse and Flechais (2005) noted that the situation is further complicated by additional aspects related to human factors including:

- A lack of understanding on behalf of employees about the importance of the data, software and systems within an organisation
- Ignorance about the level of risk attached to the assets for which they have direct responsibility for and
- A lack of understanding about how their behaviour could be putting the same assets at risk (Sasse & Flechais, 2005).

EXAMINING THE INSIDER THREAT

Establishing the Concept of 'an Insider'

In any system that incorporates an aspect of human activity the concept of 'insider threat' has the potential to impact on that system. In recent years the concept of insider threat has garnered more attention, presenting a growing concern for the internal security of organizations (Greitzer, Kangas, Noonan, & Dalton, 2010; Greitzer et al., 2016; Keeney, 2005; Probst, Hunker, Gollmann, & Bishop, 2010). In the context of businesses, the threat from an insider is multifaceted and can related to breaches in security, effects on the outward prestige of the company, and related financial loss (CPNI, 2013).

Defining a workable framework for insider threat in the context of cyber systems has proven problematic. Bishop and Gates (2008) noted a great deal of disagreement surrounding the definitions of what constitutes an insider threat. They pointed out that such a lack of consistency has the effect of preventing the development of a clear theoretical framework for investigating such an issue. With this view in mind, Bishop and Gates (2008) suggested that a unified approach would allow clearer and more effective methods for the detection of such threats. Moreover, the problematic nature of this area is further compounded when questions about what should be seen as "inside" and what elements remain "outside" of the threat perimeter are considered.

The label of insider threat makes an erroneous assumption that there is a clearly defined 'inside' within which any particular threat can be clearly encapsulated. The parameters that contribute to the notion of an insider become further blurred when viewed against the backdrop of modern working practices. This is particularly salient in instances where companies are increasingly outsourcing aspects of work to subcontractors or where the use of mobile computing allows any number of external bodies access to systems outside the physical sphere (Bishop & Gates, 2008).

In order to provide a theoretical framework for further discussion, the following section presents a brief overview of the research exploring the malicious insider threat. This is contrasted to threats based on ignorance, lack of education, and awareness, or the commonly referred to accidental or unintentional insider threat.

The Malicious Insider

Much of the research literature on the insider threat focuses on the view that these are individuals who have deep-seated malicious intent, and are conducting covert activities for financial and personal gain. For example, the definition presented by Cappelli, Moore, and Silowash (2012) is:

A current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. (p. xiii)

The research exploring the underlying psychology of the malicious insider is based, for the most part, on a small number of case studies in which the insider threat has been caught. For example Cappelli,

Moore, and Trzeciak, (2012) explored findings from ten case studies. Other researcher, such as Shaw, Ruby, and Post (1998) had previously identified four core indicators for an individual to becoming an insider threat, these included:

1. **Negative Life Experiences**: In this instance the individual expresses their disgruntlement with set-backs in their life through overt displays of anger which are directed towards both peers and those in positions of authority. The individual also presents a low threshold for frustration which is also overtly manifest through aggressive outburst.
2. **Lack of Social Skills and Isolation**: Insiders are assumed to demonstrate a lack of social skills and also exhibit a tendency for social isolation. There is some suggestion here that an *a priori* lack of social skills may preclude the individual in question to becoming isolated, which in turn may lead them to pursue such interactions in other ways such as through online social networking. This heavy reliance on computer-mediated forms of communication means that such individuals are unable to deal with social/emotional issues encountered in workplace situations effectively. As suggested by Shaw et al. (1998) a combination of these elements could lead to the individual retaining feelings of frustration and disgruntlement. This in turn could be overtly viewed in difficult social interactions with peers and work colleagues as well as what is termed "emotional leakage", outbursts that are of a magnitude that far outweigh the nature of the incident.
3. **Sense of Entitlement:** Insiders are proposed to suffer from a sense of entitlement, usually afforded to them via special privileges or access rights they have been permitted in pursuit of their duties. The individual may possess a special skill set that allows them to leverage such special treatment and may be further manifest through poor treatment of peers whom they may view as inferior. They may also have difficulty in adapting to specific rules or protocols that have been put into place by the organisation, perhaps fitting into the Proprietors category highlighted earlier.
4. **Ethical Flexibility:** This is another area in which insiders are deemed to exhibit some degree of underdevelopment. This notion means that insiders may suffer from an inability to empathize with colleagues or others that would usually prevent an individual from engaging in acts of insider threat. Such immaturity is also linked to a breakdown in the inhibitory processes that control emotional outbursts in aspects such as aggression.

Findings from the CPNI (2013) report added some more specific detail to the personality traits that have been associated with those who have committed insider threat. In the context of the CPNI report insider threat was defined as 'a person who exploits, or has the intention to exploit, their legitimate access to an organisation's assets for unauthorised purposes' (p. 4). This study explored 120 UK-based case studies on insider threat, and collated those key elements that had a significant impact on behaviour as well as others within the environment. These personality traits are summarised as:

- **Immaturity:** The individual is seen to lack in overall life experience and falls into the category of being "high maintenance" in terms of the attention and guidance they require; also have clear difficulties in making critical life decisions.
- **Low Self-Esteem**: Lacks confidence in social situations and has a heavy dependence on recognition and praise from others; finds it hard to cope with adverse social situations, criticism and tasks that fall outside of their comfort zone.

- **Amoral and Unethical**: The individual lacks any clear understanding of morality and shows no remorse for their behaviour, particularly in terms of the effect this may have on others.
- **Superficial**: The majority of insiders lack a clear sense of self and identity, presenting someone that is described as being "hard to know" by peers and colleagues.
- **Restless and Impulsive**: A common element that crops up in a variety of places when discussing the nature of the insider's personality. Individual is seen to require constant stimulation and also is highly hedonistic (the requirement to seek pleasure above all other needs is apparent in someone with a hedonistic personality).
- **Lacks Conscientiousness:** Has a disregard for established rules and practices; clearly neglects workplace duties and responsibilities; poor attention to detail, poor judgement and a lack of focus.
- **Manipulative:** Uses their skills of persuasion to get their own way and will garner relationships that will serve to nurture their own self-interest. Also seen to adopt a social position that aids in serving their own needs, such as being agreeable and compliant to those in position of power.
- **Emotionally Unstable:** Prone to a variety of exaggerated mood swings and overt over reactions to problems; appears to complain about the most trivial of incidents.
- **Evidence of Some Underlying Psychological or Personality Disorder:** The CPNI report is vague about this aspect with little specific details on this aspect of the personality profile for the Insider, or indeed how this aspect was measured in their study.

Further to this, the CPNI report also highlights situational aspects that are evident in the psychosocial environment of the insider. These elements are split into two underlying categories:

- "Lifestyle changes" which are related to a change in personal circumstances and thus a change in experienced levels of stress.
- "Circumstantial vulnerabilities" which in the context of the CPNI report refer to "work, profile or personal issues that could make an individual vulnerable" (p.11).

The CPNI report presents a number of key predictors, based on aspects of the individual's life experiences and psychological factors, viewed as being of critical importance in the development of a potential insider threat. These are:

- **Demonstrating Poor Work Attitude:** A failure to follow accepted protocol or to read important documentation about new procedures or operating instructions.
- **Shows Signs of Being Stressed:** Overt symptoms of stress that include loss of temper, apathy (burnout), increase in nervous habits (ticks, aspects of OCD), problems with memory and concentration, evidence of confusion, difficulty in making decisions.
- **Exploitable or Vulnerable Lifestyle:** Has an element of their lifestyle which allows them to be exploited by an external force or agent e.g. serious financial stress, alcohol abuse, drug addiction, gambling – each of these could lead to a strong desire for financial gain.
- **Exploitable or Vulnerable Work Profile:** The individual's position within the company allows them access to highly prized or sought-after assets which in turn could be marketed for profit
- **Recent Negative Life Events:** A variety of elements could be included here, such as problems at work, loss of status (socially and work), personal injury, bereavement, relationship breakup, financial difficulty or loss.

However, these concepts are only directly applicable to those attacks accompanied by a level of intentionality or direct motive. Other researchers have argued against the overarching label of 'insider threat' and moved towards a more flexible term of insiderness (Bishop, Gollmann, Hunker, & Probst, 2008; Hunker & Probst, 2011). These researchers have argued that insider threat is more adequately represented in the form of a continuum rather than a dichotomy. Hunker and Probst (2011) compared the actions of an accidental insider to that of a 'real insider', with the latter being the group of individuals who exhibit malicious intent in their exploits. This real insider group also poses a great deal of skill and expertise, which could include knowledge related to programming, IT infrastructure and company systems that allow for a more holistic view of the attack landscape. At the opposite end of the continuum there are the accidental or unintentional insiders, who may have limited knowledge of accepted security protocols, their actions are obvious, and they make no direct attempt to cover up their mistakes. It is these 'accidental insiders' who present the focus for this current chapter, alongside an examination of how individual differences could make certain people more prone to lapses in cybersecurity.

The Accidental or Unintentional Insider

In order to account for incidences of unintentional insider threat (UIT; CERT, 2013) a further definition was presented:

An unintentional insider threat is a current or former employee, contractor, or business partner who has or had authorized access to an organization's network, system, or data and who, through action or inaction without malicious intent, causes harm or substantially increases the probability of future serious harm to the confidentiality, integrity, or availability of the organization's information or information systems. (CERT, 2013, p. ix)

This definition for UIT focuses directly on threat as a result of inaction or indeed a specific lack of knowledge on the behalf of the individual alongside the lack of actual intent to cause harm. Thus, the key components to the conceptualization of UIT are elements of human failure or limitations related to human performance (CERT, 2013). This has the potential to include mistakes made though time pressures exerted as a result of a job, the level of task difficulty, a lack of knowledge, and cognitive factors such as inattention (CERT, 2013). Examples of unintentional insider threat presented by CERT (2013) included the accidental disclosure of sensitive information (either via website, email or fax); an individual devolving log-in details (password and username) as a result of social engineering or via malware/spyware; the improper disposal of physical records; and the loss of information through the misplacement of portable equipment including smartphones, USB drives, CDs and hard drives. These random acts are of greater potential concern for organizations as they typically have no motive, no direct intent and no prior indicators upon which to act. Unfortunately, the end result is still the same, and the actions of the unintentional insider can be as damaging as those perpetrated by the malicious attacker.

The concept of UIT presents another perspective from which researchers and security professionals can begin to explore the potential threats presented in any system that incorporates humans. The CERT (2014) report noted that over 40% of computer and organizational security professionals believed accidental insiders were the greatest potential source of risk. However, to date, very few attempts have been made to examine how aspects of human factors serve to influence the potential for UIT. This may

be in part due to a lack of research focus or the belief that technical solutions alone can provide the mitigation for such.

The rest of this chapter will focus on exploring how a better understanding of underlying human factors could influence aspects of cybersecurity. The first part will explore research that attempted to develop effective scales in order to assess the individual's adherence to effective cybersecurity principles alongside key psychological traits.

Assessing Information Security Behaviors

A variety of attempts have been made to create effective scales designed to record aspects individual adherence to cybersecurity protocols. For the most part these have been deployed in work-based environments, with a respective gap in scales being developed for younger populations and individuals not in employment. It has also been noted that many previous scales have a very narrow focus and explore just one aspect of cybersecurity such as passwords (Stanton et al. (2005), mobile computing (Mylonas et al., 2013) and specific security features of key applications (Furnell et al., 2006; Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

Siponen, Pahnila, and Mahmood (2010) presented one recent attempt to produce a scale that was designed to explore individual attitudes towards information security. The focus of this study was to examine key reasons why certain employees were more likely to comply with the cybersecurity polices of the organization. Their findings suggested that the existence of social pressure from both peers and superiors within their organization influenced the potential for adherence to such policies. It was noted that if peers and superiors have a positive cybersecurity posture this would in turn permeate throughout the organization to its other members. The individual's self-efficacy in the context of cybersecurity was also shown to be a key determiner in their capacity to engage in effective cyber inoculation. For example, Siponen et al. (2010) present the instance of an individual who unwittingly sends confidential information out through email without encrypting it. According to Siponen et al. (2010) the individual must have the knowledge or capacity to encrypt this information before they can actually engage in that behavior. From this regard, if the individual has no awareness of the security policies of the organization, they cannot align to them, and hence are in danger of contravening them through ignorance and misunderstanding. However later researchers noted that the items used within the scale produced by Siponen et al. (2010) were very basic in nature and had the potential to produce an inherent bias, thus leading to an overall underestimation of the current security issues being faced within organisations (McCormac, Parsons, Zwaans, Butavicius, & Pattinson, 2016).

Egelman and Peer (2015a, 2015b) presented the development of the Security Behavior Intention Scale (SeBIS) that comprised of 16-items designed to assess adherence to information security advice. The SeBIS included 4 key sub-scales that measured attitudes towards password generation, securing digital devices, engaging in proactive awareness and updating software. In their initial testing, the researchers explored the relationship of security behaviors to a variety of psychological constructs. These included:

- **Domain-Specific Risk-Taking Scale** (DoSpeRT; Blais & Weber, 2006):
  - A measure that explores the capacity to engage in risk taking behaviours across five key areas including ethical, financial, health and safety, recreational and social.
- **General Decision-Making Style** (GDMS; Scott & Bruce, 1995):

  - A measure for how people approach decision-making in association with five dimensions that include rationality, avoidance, dependence, intuition and spontaneity.
- **Need for Cognition** (NFC; Cacioppo, Petty, & Feng Kao, 1984):
  - This is an individual's preference or tendency to engage in and gain pleasure from cognitively effortful activities.
- **Barratt Impulsiveness Scale** (BIS; Patton, Stanford, & Barratt, 1995):
  - Explores impulsivity on three dimensions related to non-planning, attention and motor impulsiveness.
- **Consideration for Future Consequences** (CFC; Joireman, Shaffer, Balliet, & Strathman, 2012):
  - This scale measures the individual's capacity to consider potential future outcomes for their present actions.

The results from initial testing using the SeBIS demonstrated a variety of relationships with the above measures. Each of the four sub-scales for the SeBIS correlated positively with inquisitiveness as measured by the need for cognition scale. Individuals who exhibit higher levels of NFC are perhaps more questioning details of their daily life which could impact their cybersecurity, and this inquisitiveness leads them to investigate and explore rather than ignore or accept. Similarly, a consideration of the consequences of their actions (as measured through the CFC) also showed positive correlations with the four sub-scales of the SeBIS. The authors of the report suggested that a more active engagement in cybersecurity is linked directly to a capacity to assess how their current decisions may affect their future. This maps well onto the finding that the three subscales of the BIS, which measures impulsivity, were negatively correlated with security sub-scales measured on the SeBIS; those individuals who are quick to act or lack impulse control are those who may quickly respond to a spam email or phishing attack. Aspects of decision-making also demonstrated correlations with a number of sub-scales from the SeBIS. For instance, the rational sub-scale of the GDMS showed a positive correlation with aspects of password protection, general security awareness and updating software. The concept of rationality has been linked to a deliberate and logical approach to decision-making, and it has also been noted that those individuals who have a rational approach to decision-making are more likely to assume a personal responsibility for decision that affect them (Scott & Bruce, 1995). The avoidant decision-making type, typified by an individual who puts off or procrastinates about making decisions was negatively correlated to each of the four sub-scales from the SeBIS. There was an associated link between the dependence style of decision-making and scores on the SeBIS too, with those less likely to need help or assistance in their decision-making having a higher level of overall security awareness. Egelman and Peer (2015b) suggested that those individuals who were more proactive about their security had a less of a capacity to rely on others for information.

In the context of the present discussion the findings from Egelman and Peer (2015a, b) provided one of the first attempts to assess how individual differences could have a direct impact on their cybersecurity behaviors. It would appear that those individuals who are more inquisitive, more rational and less prone to procrastination in decision-making represent those more likely to engage in effective cybersecurity behaviors. The benefits of knowing such information presents the theoretical possibility of system design with such differences in mind. This could potentially allow the implementation of system messages and warnings that are tailored to the individual, hence presenting a more targeted mitigation to poor cybersecurity behaviors.

The SeBIS was later employed in further research by Tischer et al. (2016) who examined the potential for individuals to plug in USB devices that had been littered around a university campus. This strategy is often presented as a key mechanism for infiltration used by social engineers who leave such devices in prominent places in an attempt to gain entry to highly protected systems (Tischer et al., 2016). The pathway to gaining access is via the device, which is usually loaded with malware allowing the social engineer remote access to system once it has been plugged into a networked computer. In contrast to Egelman and Peer's work, Tischer et al. (2016) found that individuals who were more likely to plug in a USB device were no risker when compared to a matched sample. In fact, those individuals who did plug in the USB were more risk averse in all categories apart from that of recreational risk. However it appears that individuals devolve responsibility for their protection of the computer and security measures deployed on it, or are ignorant of the risks attached to poor cybersecurity practices (Tischer et al., 2016). Tischer et al. (2016) also used the SeBIS, but noted that the internal reliability of the scale was found to be much lower than had originally been found in the original research by Egelman and Peer (McCormac et al., 2016).

One of the most recently developed scales designed to explore the information security of individuals is the Human Aspects of Information Security Questionnaire (HAIS-Q; (Parsons et al., 2017, 2014). The HAIS-Q comprises of a variety of items that assess three key elements in the context of cybersecurity; these are knowledge, attitude and behavior. The underlying structure of the HAIS-Q examines these constructs in 5 core areas including password management, email use, Internet use, Social networking, incident reporting, mobile computing and information handling (Parsons et al., 2014). Higher scores on the HAIS-Q indicate a good awareness of information security, whilst a lower score demonstrates lack of knowledge as well as the propensity to engage in potentially risky activities, e.g. sharing passwords. The HAIS-Q has undergone an impressive amount of testing across a broad spectrum of populations establishing a robust test-retest reliability in the process (see Parsons et al., 2017).

In the context of exploring individual differences in security behaviors, the HAIS-Q was paired with key demographic and personality factors in a study by McCormac, Zwaans, et al., (2016). Scores on the HAIS-Q were shown to differ significantly across age groups, with the overall observation being that those in the older age groups demonstrated higher overall scores for information security. In order to assess if this relationship was influenced by age-related differences in risk taking behaviors, the researchers controlled for this and noted that the correlation between age and scores on the HAIS-Q persisted, although were slightly weaker. A gender difference between males and females was also noted, with females presenting significantly higher scores on the HAIS-Q compared to males, although the authors noted that the effect size for such a result was small. So in this instance age and gender both present as potential sources for individual differences in cybersecurity-related behaviors. The unknown element here is if these sources for variance in cybersecurity can be accounted for, and if effective system design could serve to isolate and mitigate the impact from such.

The work by McCormac et al. (2016) also included an exploration of how personality traits and a measure of risk taking were associated with scores on the HAIS-Q. The study used the five-factor model of personality, with the most frequently cited version used being that by John and Srivastava (1999), shown in Table 1.

A significant positive relationship between the personality traits of agreeableness, openness and conscientiousness with scores on the HAIS-Q were observed from the research by McCormac et al. (2016). Furthermore, a negative correlation was noted between risk-taking and scores on the HAIS-Q, with those less likely to engage in risky behaviors having higher overall scores. These findings were

Table 1. The five-factor model of personality as taken from John and Srivastava (1999; p.121)

Factor Name	Description
Extraversion	An energetic approach to the social and material world and incudes traits such as sociability, activity, assertiveness, and positive emotionality.
Agreeableness	Contrasts a prosocial and communal orientation towards others with antagonism and includes traits such as altruism, tender-mindedness, trust and modesty.
Conscientiousness	Socially prescribed impulse control that facilitates task and goal oriented behavior, such as thinking before acting, delaying gratification, following norms and rules, and planning, organizing, and prioritizing tasks.
Neuroticism	Contrasts emotional stability and even-temperedness with negative emotionality, such as feeling anxious, nervous, sad, and tense.
Openness	In contrast to closed-mindedness, describes the breadth, depth, originality, and complexity of an individual's mental and experiential life.

noted as being in partial agreement with previous research (Pattinson et al., 2015) which also found that aspects of agreeableness, conscientiousness and openness served to explain the most variance in information security behaviors (McCormac, Zwaans, et al., 2016).

The research reviewed above provides a wide and somewhat contrasting basis for examining human factors in the context of cybersecurity. It would appear that there is some commonality in the findings that have examined self-reported cybersecurity knowledge, attitudes and behaviors. Predominately, individual differences in aspects of personality have the potential to predict to what level that individual will engage in information security behaviors. It appears that those who are more conscientious, open, agreeable, risk adverse and rational are those more likely to positively engage in effective cybersecurity behaviors. Alongside these personality traits it would also appear that both age and gender also serve as important moderators of active information security behavior further complicating issues.

SOLUTIONS AND RECOMMENDATIONS

Mitigating the threat posed by the accidental insider is, on the face of it, not easily accomplished. There is often an assumption made that those aspects of employee behavior which serve to create a level of risk for the organization relates directly to a lack of understanding (Coventry, Briggs, Jeske, & Van Moorsel, 2014). The sheer scope of information security behavior that need to be enhanced, modified or altered provide a clear challenge for any awareness campaign. The list is long and there is no potential 'one-size fits all' approach which could effectively be applied to bring awareness for just a few of these elements. These aspects can include:

- Regularly updating anti-virus software.
- Using only trusted and secure connections, including Wi-Fi.
- Updating existing software.
- Awareness of physical surroundings (e.g. preventing shoulder surfing).
- Reporting suspicious behaviour.
- Keeping up-to-date with current threats.
- An awareness of trusted sites and services.

- Ensuring passwords are strong enough.
- Limiting the amount of personal information being shared online (Coventry et al., 2014).

In order to overcome these potential deficiencies, Coventry et al. (2014) noted that organizations often implement a wide variety of training schemes in an attempt to educate end-users (Leach, 2003). The effectiveness of these training programs is often limited to a unidirectional process where employees are presented with 'best practice', and behavioral change is attempted through the use of 'expert' advice (Coventry et al., 2014). A recent report produced by the Information Security Forum (ISF, 2014) presented a wide range of reasons as to why security awareness training failed to fully engage the human participant within the process. These key points included:

1. Solutions are not aligned to the business risks.
2. Neither progress nor value is measured.
3. Incorrect assumptions are made about people and their motivations.
4. Unrealistic expectations are set.
5. The correct skills are not deployed.
6. Awareness is just background noise (ISF, 2014: 1).

For many individuals it would appear that awareness training becomes an unnecessary burden that must be completed as part of their daily work lives. If expectations placed on the individual employee are also set too high, and the capacity to deploy the skills they have learned is stifled, there is a potential for both time and resources to be wasted.

The actual way in which such awareness training is conveyed can also have a significant impact on its effectiveness for eliciting a change in behavior. For example, Khan, Alghathbar, Nabi, and Khan (2011) noted that educational/academic presentations and group-based discussions served to enhance the knowledge, attitude, intention to engage and behaviors of those studied. Other forms of communication, such as emails, newsletters, videogames, posters and computer-based training all had limited effectiveness in terms of getting individuals to change their behaviors and engage in more effective security activities (Khan et al., 2011).

A variety of attempts have been made to utilize behavioral change mechanisms in the context of cybersecurity (Coventry et al., 2014; Jeske, Coventry, & Briggs, 2013; Turland, Coventry, Jeske, Briggs, & van Moorsel, 2015). However, it is noted that these attempts are exceptions rather than the norm. Other researchers have pointed out that there is a potential to use aspects of behavioral economics as a mechanism for eliciting behavioral change (Briggs, Jeske, & Coventry, 2016). Behavioral economics is starkly contrasted to the standard economic model in terms of human decision making and behavior, with the latter asserting that an individual is fully rational when engaged in decision making and is always mindful of the consequences for their actions (Briggs et al., 2016). The standard economic model has appeared at be an idealistic view of human information processing and has failed to adequately explain the actual behaviors of individuals in any number of key settings. Behavioral economics on the other hand adopts a more pragmatic approach by highlighting several key principles proposed to account for the irrationality of human behavior. This work was formalized in the work of Thaler and Sunstein (2008), which presented the basis for exploring how predictable deviations from rational processes could in turn be used to 'nudge' an individual towards a more desirable decision (Briggs et al., 2016).

The MINDSPACE framework, originally developed by Dolan et al. (2012) has been used by a variety of researchers to capture the key influencers for behavioral change. These elements are included in Table 2.

Coventry et al. (2014) used the MINDSPACE framework provided by Dolan et al., as a basis for creating a set of behavioral nudges to prevent individuals from choosing insecure wireless networks. The researchers highlighted a series of possible nudges aligned to specific scenarios that could be used in a practical way. For example, in the instance of Messenger, the behavioral nudge was to present a warning message from a trusted provider and not from a generic source. The researchers even suggested the possibility of having a celebrity to provide the warning message, but this may only work if the individual is both well respected and well known. In the final testing of the framework, Coventry et al. (2014) opted to use an affective nudge by changing both the color and order of the available wireless networks. Those wireless networks that were deemed safe and secure appears in green towards the top of the list, with unsecure networks appearing lower down the list in red. Jeske et al. (2014) presented the results of this research, with these affective cues presented as an effective mechanism for helping individuals choose a more secure network. However, the researchers also noted that individual differences in the characteristics of users (such as proficiency with IT and poorer impulse control) also led to poorer security decisions, with nudges presenting an effective mechanism for changing the behavior of those with poor impulse control. To date this represents one of the few published empirical tests of behavioural nudges in an information security context, but focuses rather narrowly on just one element from the MINDSPACE framework.

In a final point, Bada, Sass, and Nurse (2014) suggested a series of key aspects that should be considered when designing cyber security awareness campaigns. These key points included:

1. Security awareness training has to be professionally organized and prepared if it is to work – ad hoc training courses and inconsistency in the messages being conveyed will confuse the end user.
2. The use of fear as an effective strategy to create change is not recommended, and there is potential that it could instil a sense of fear in those who can ill afford to take risks.
3. Security education needs to be targeted and needs to be practical in nature – it needs to give the individual a concrete and achievable goal or action, which is in turn measurable and allows feedback to be provided.

Table 2. The MINDSPACE framework for behavior change

MINDSPACE cue	Behavior
Messenger	We are heavily influenced by who communicates information to us
Incentives	Our responses to incentives are shaped by predictable mental shortcuts such as strongly avoiding losses
Norms	We are strongly influenced by what others do
Defaults	We 'go with the flow' of pre-set options
Salience	Our attention is draw to what is novel and seems relevant to us
Priming	Our acts are often influenced by sub-conscious cues
Affects	Our emotional associations can powerfully shape our actions
Commitments	We seek to be consistent with our public promises, and reciprocate acts
Ego	We act in ways that makes us feel better about ourselves.

(from Dolan et al., 2012, p. 266)

4. Change needs to be sustainable and continuous – once you have the atmosphere to illicit change, this needs to be exploited and feedback should be provided throughout this period.
5. Cultural contexts should be considered whenever cyber security awareness campaigns are being designed – there is not a one-size fits all approach that will work, and cultural nuances need to be taken into consideration

FUTURE RESEARCH DIRECTIONS

There are multiple directions in which future research could be taken, and a point that becomes apparent when exploring the available literature in this area is that the contribution human factors can make to cybersecurity is only just gaining a significant focus. A consistent and directed approach to exploring how aspects of human factors can serve to influence (and therefore also be targeted in order to mitigate) risk within any system is inherently important. In a similar way, the actual mechanisms used to bring awareness to individuals for effective cybersecurity behaviors also needs to be researched. The following present some key areas for further research, but the scope of the area is overwhelming and deserves a more in-depth discussion than is currently possible.

Behavioral Nudges and ISA

The work by Dolan et al., (2012) in the development of the MINDSPACE framework for behavioral nudges presents a clear pathway for future exploration. A number of researchers have already noted that affective nudging techniques can serve as key mechanisms for eliciting more effective information security awareness (Coventry et al., 2014; Jeske et al., 2013; Turland et al., 2015). However much of this research does focus solely on the affective elements presented in the MINDSPACE framework, meaning that there is an even greater number of potential routes to follow for influencing behavioral change. It may be the case that using a number of key elements from the MINDSPACE framework could create more effective information security strategies, and by adding or subtracting various components, behavioral changes could be enhanced. It is evident that more detailed empirical research is needed in this area in order for such questions to be answered.

Individual Differences and Information Security

Individual differences in the context of information security and accidental insiderness could also provide another avenue for further research. As reviewed in this current chapter, there has been some clear attempts to highlight how individual differences can serve to influence attitudes and adherence to information security. Aspects such as poor impulse control, knowledge of IT and elements of personality have all been linked to information security behaviors. However, there are a huge amount of potential avenues that have been, to date, left unexplored and would provide a useful metric to not only measure ISA against, but also map potential behavioral nudges onto.

One area that has so far escaped in-depth exploration in the context of human factors in cybersecurity is those elements that lie outside of traditional 'trait based' personality factors. These factors link into the artifacts of modern life, and span a plethora of phenomena associated with the use of digital technology. For instance, there has been some discussion of how aspects such as cyberloafing and Internet

addiction could both influence ISA (for example see Hadlington, 2017; Hadlington & Parsons, 2017). The term cyberloafing has also been used to describe a process through which individuals actively engage the use of the companies' Internet access during work hours for non-work related purposes (Ozler & Polat, 2012). Blanchard and Henle (2008) defined the concept of cyberloafing as "employees' voluntary nonwork-related use of company provided email and Internet while working (p. 1068). With the prevalence of cyberloading being noted as being widespread in employment (Malachowski, 2005), exploring how ISA is affected by individuals engaging in cyberloafing provides another useful measure of how accepted social norms in the context of work-based use of information technology impacts on cybersecurity. Further work to expand on these findings, and to examine other associated variables, is deemed critical to move the field forward.

CONCLUSION

As noted in this chapter, exploring the role of the human element within the context of any cybersecurity is complex, multifaceted, and presents a potential conundrum to any security professional attempting to secure systems. The threats from the accidental insider, whether it is through ignorance, lack of attention, or human error is quickly becoming a growing concern to security professionals. Unlike malicious attacks from internal and external agents, the impact that UIT has is far harder to detect and mitigate but is potentially just as damaging. Movements towards a clearer understanding of how crucial aspects related to human factors have been made, but progress in this area is slow, fails to keep up with the constant evolution of the threat landscape, and is lacking a clear theoretical framework. Further work needs to be done in this area if we are to develop a clearer understanding of how human factors interact in the cybersecurity landscape. A focus not just on how these factors impact on business cybersecurity, but also personal cybersecurity is also important, and examining how these two aspects interact would also appear to be an aspect for future research. It is also apparent that current research on mitigating risks suggests that a 'one-size-fits-all' approach to preventing lapses in cybersecurity is not currently working. More work focusing on why mitigating threats from human actors within the system is so difficult would appear to be urgently needed. Aligned to this, appropriate interventions need to be designed from the ground up, with a clear focus on their effectiveness rather than a 'fire and forget' attitude where there is no follow up to explore if they have worked.

REFERENCES

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2016). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior*, *69*, 437–443. doi:10.1016/j.chb.2016.12.040

Bada, M., Sass, A. M., & Nurse, J. R. C. (2014). *Cyber Security Awareness Campaigns Why do they fail to change behaviour?* Academic Press.

Bishop, M., & Gates, C. (2008). Defining the insider threat. In *Proceedings of the 4th annual workshop on Cyber security and information intelligence research* (pp. 12–14). New York: ACM Press. doi:10.1145/1413140.1413158

Bishop, M., Gollmann, D., Hunker, J., & Probst, C. W. (2008). Countering insider threats. In *Dagstuhl Seminar Proceedings 08302* (pp. 1–18). Academic Press. Retrieved from http://vesta.informatik.rwth-aachen.de/opus/volltexte/2008/1793/pdf/08302.SWM.1793.pdf

Blais, A.-R., & Weber, E. U. (2006). A Domain-Specific Risk-Taking (DOSPERT) scale for adult populations. *Judgment and Decision Making*, *1*(1), 33–47. doi:10.1037/t13084-000

Briggs, P., Jeske, D., & Coventry, L. (2016). Behaviour change interventions for cybersecurity. In L. Little, E. Sillence, & A. Joinson (Eds.), *Behaviour Change Research and Theory; Psychological and Technological Perspectives*. New York: Academic Press.

Cacioppo, P., Petty, R., & Kao, F. C. (1984). The Efficient Assessment of Need for Cognition. *Journal of Personality Assessment*. doi:10.1001/archpsyc.64.10.1204

Cappelli, D., Moore, A., & Silowash, G. (2012). *Common Sense Guide to Mitigating Insider Threats* (4th ed.). Academic Press. Retrieved from http://www.stormingmedia.us/00/0055/A005585.html

Cappelli, D., Moore, A., & Trzeciak, R. (2012). *The CERT Guide to Insider threats*. Academic Press.

CERT. (2013). *Unintentional insider threats: A foundational study*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Unintentional+Insider+Threats+:+A+Foundational+Study#0

CERT. (2014). *Unintentional Insider Threats: Social Engineering*. Retrieved from http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA592507

Coventry, L., Briggs, P., Jeske, D., & Van Moorsel, A. (2014). SCENE: A structured means for creating and evaluating behavioral nudges in a cyber security environment. Lecture Notes in Computer Science, 8517, 229–239. doi:10.1007/978-3-319-07668-3_23

CPNI. (2013). *CPNI Insider Data Collection Study: Report of Main Findings.* London: CPNI.

Dolan, P., Hallsworth, M., Halpern, D., King, D., Metcalfe, R., & Vlaev, I. (2012). Influencing behaviour: The mindspace way. *Journal of Economic Psychology*, *33*(1), 264–277. doi:10.1016/j.joep.2011.10.009

Egelman, S., & Peer, E. (2015a). Predicting Privacy and Security Attitudes. *Computers and Society: The Newletter of ACM SIGCAS*, *45*(1), 22–28. doi:10.1145/2738210.2738215

Egelman, S., & Peer, E. (2015b). Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS). *Proceedings of the ACM CHI'15 Conference on Human Factors in Computing Systems*, *1*, 2873–2882. doi:10.1145/2702123.2702249

Greitzer, F., Kangas, L., Noonan, C., & Dalton, A. (2010). *Identifying at-risk employees: A behavioral model for predicting potential insider threats*. Retrieved from http://www.pnl.gov/main/publications/external/technical_reports/PNNL-19665.pdf

Greitzer, F. L., Imran, M., Purl, J., Axelrad, E. T., Leong, Y. M., & Becker, D. E. … Sticha, P. J. (2016). Developing an ontology for individual and organizational sociotechnical indicators of insider threat risk. *CEUR Workshop Proceedings*, 19–27.

Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon (London)*, *3*(7), e00346. doi:10.1016/j.heliyon.2017.e00346 PMID:28725870

Hadlington, L., & Parsons, K. (2017). Can Cyberloafing and Internet Addiction Affect Organizational Information Security? *Cyberpsychology, Behavior, and Social Networking*, *20*(9), 567–571.

Hunker, J., & Probst, C. (2011). Insiders and insider threats—an overview of definitions and mitigation techniques. *Journal of Wireless Mobile Networks, Ubiquitous Computing and Dependable Applications*, *2*(1), 4–27. Retrieved from http://isyou.info/jowua/papers/jowua-v2n1-1.pdf

Information Security Forum. (2014). *From Promoting Awareness to Embedding Behaviours - Secure by choice, not by chance, Abstract*. Author.

Jeske, D., Coventry, L., & Briggs, P. (2013). Nudging whom how : IT proficiency, impulse control and secure behaviour. *CHI Workshop on Personalizing Behavior Change Technologies 2014*.

John, O. P., & Srivastava, S. (1999). Big Five Inventory (Bfi). Handbook of Personality: Theory and Research, 2, 102–138. doi:10.1525/fq.1998.51.4.04a00260

Joireman, J., Shaffer, M. J., Balliet, D., & Strathman, A. (2012). Promotion Orientation Explains Why Future-Oriented People Exercise and Eat Healthy: Evidence From the Two-Factor Consideration of Future Consequences-14 Scale. *Personality and Social Psychology Bulletin*, *38*(10), 1272–1287. doi:10.1177/0146167212449362 PMID:22833533

Keeney, M. (2005). *Insider threat study: Computer system sabotage in critical infrastructure sectors*. Retrieved from http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Insider+Threat+Study+:+Computer+System+Sabotage+in+Critical+Infrastructure+Sectors#0

Khan, B., Alghathbar, K. S., Nabi, S. I., & Khan, M. K. (2011). Effectiveness of information security awareness methods based on psychological theories. *African Journal of Business Management*, *5*(26), 10862–10868. doi:10.5897/AJBM11.067

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), 685–692. doi:10.1016/S0167-4048(03)00007-5

Malachowski, D. (2005). Wasted Time At Work Costing Companies Billions. *Asian Enterprise*, 14–16.

McCormac, A., Parsons, K., Zwaans, T., Butavicius, M., & Pattinson, M. (2016). *Test-retest reliability and internal consistency of the Human Aspects of Information Security Questionnaire* (HAIS-Q). Academic Press.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2016). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156. doi:10.1016/j.chb.2016.11.065

Nurse, J. R. C., Creese, S., Goldsmith, M., & Lamberts, K. (2011). Trustworthy and effective communication of cybersecurity risks: A review. *Proceedings - 2011 1st Workshop on Socio-Technical Aspects in Security and Trust, STAST 2011*, 60–68. doi:10.1109/STAST.2011.6059257

Ozler, D. E., & Polat, G. (2012). Cyberloafing phenomenon in organizations: determinants and impacts. *International Journal of eBusiness and eGovernment Studies, 4*(2), 1–15. Retrieved from http://www.sobiad.org/eJOURNALS/journal_IJEBEG/arhieves/2012_2/derya_ergun.pdf

Parsons, K., Calic, D., Pattinson, M., Butavicius, M., McCormac, A., & Zwaans, T. (2017). The human aspects of information security questionnaire (HAIS-Q): Two further validation studies. *Computers & Security*, *66*, 40–51. doi:10.1016/j.cose.2017.01.004

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176. doi:10.1016/j.cose.2013.12.003

Patton, J. H., Stanford, M. S., & Barratt, E. S. (1995). Patton Factor Structure of the BIS.pdf. *Journal of Clinical Psychology*.

Pfleeger, S. L., & Caputo, D. (2012). Leveraging Behavioral Science to Mitigate Cyber Security Risk Security Risk. *Computers & Security*, *31*(4), 597–611. doi:10.1016/j.cose.2011.12.010

Probst, C., Hunker, J., Gollmann, D., & Bishop, M. (2010). *Insider Threats in Cyber Security. Vasa*. New York: Springer. doi:10.1007/978-1-4419-7133-3

Sasse, M., Brostoff, S., & Weirich, D. (2001). Transforming the "weakest link": A Human-Computer Interaction Approach for Usable and Effective Security. *BT Technology Journal*, *19*(3), 122–131. doi:10.1023/A:1011902718709

Sasse, M., & Flechais, I. (2005). *Usable Security: Why Do We Need It? How Do We Get It?* Retrieved from http://discovery.ucl.ac.uk/20345/

Scott, S., & Bruce, R. (1995). Decision-making Style: The Development and Assessment of a New Measure. *Educational and Psychological Measurement*, *55*(5), 818–831. doi:10.1177/0013164495055005017

Shaw, R., Ruby, K., & Post, J. (1998). The Insider Threat to Information Sytems. *Security Awareness Bulletin*, 2–98.

Siponen, M., Pahnila, S., & Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. *Computer*, *43*(2), 64–71. doi:10.1109/MC.2010.35

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., & Bailey, M. (2016). Users Really Do Plug in USB Drives They Find. *IEEE Symposium on Security and Privacy*, 1–14. doi:10.1109/SP.2016.26

Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A. (2015). Nudging Towards security: Developing an Application for Wireless Network Selection for Android Phones. *Proceedings of the 2015 British HCI Conference on - British HCI '15*, 193–201. doi:10.1145/2783446.2783588

Whitten, A., & Tygar, J. D. (1998). *Usability of Security: A Case Study. Computer Science*. Retrieved from http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA361032

KEY TERMS AND DEFINITIONS

Cyberloafing: Using work-based IT for non-work, personal purposes.

Insider Threat: A threat to an organisation by a former or current employee who, with malicious intent, deploys an exploit designed to either disrupt normal system functioning or exhort sensitive information for financial again.

Personality: A theoretical psychological construct that has permanence throughout the individual's life span.

Unintentional Insider Threat: The threat posed by a current employee who, without malicious intent, causes a breach in organizational cybersecurity.