# Security-Aware Organisational Cultures as a Starting Point for Mitigating Socio-Technical Risks

Sven Übelacker

Security in Distributed Applications
Hamburg University of Technology (TUHH)
Harburger Schloßstr. 20
21079 Hamburg, Germany
uebelacker@tuhh.de

**Abstract:**

This extended abstract briefly introduces Hofstede's three leveled model of human mental programming which captures the unique mental constitution of a person. These levels devide the vague "human factor" in more approachable categories. In the following sections each category is addressed and presented seperately according to research found and regarding security-aware behaviour.

By including universal human behaviour, characteristics of organisational and national cultures as well as (occupational) grouping of personality traits of employees, we might be able to identify emerging social threats. Furthermore, assessing social risks could help to develop guidelines for cultural change towards a more security-aware organisational culture.

As the influence of an organisation on external factors (other than their own organisational culture) tends to be minimal, developing, allowing, and applying cultural changes can be a promising approach in mitigating socio-technical risks.

## Keywords

Human factors, insider threat, organisational culture, security, security awareness, social engineering.

## 1 Introduction

It is becoming increasingly difficult to ignore human factors in mitigating organisational risks. Over the last decades the physical and digital domains were subject to intense security research. However, the growing deployment of new technologies like cloud services or the desired ability to use personal devices for work related tasks (*BYOD*) removed previously established security barriers. Thus, forcing us to think more in socio-technical risk management and about employees as a potential target.

An employee as a target of *Social Engineering (SE)* should be as vigilant as possible. This leads to the question if the work environment supports behaviour to not succumb to social attacks and not to become an insider threat unwillingly. Thus, attackable personnel will become an asset for security-aware organisations. Is the awareness inside an organisational culture with its communication and interaction practices sufficient against the majority of emerging threats? In which way should either the awareness training or the lived organisational culture be changed in particular aspects?

A strong relationship exists between an individual's personal factors and past events and experience as well as their cultural background, age, and gender [PJBC09]. Furthermore, human factors in information security consist of two dimensions: knowledge and human co-operated behaviour [VNvS05]. Knowledge can be addressed by employee training. Proper training for security awareness or initiatives to change the organisational security culture can be conducted after an analysis of human behaviour.

Moreover, in human history technological advance led to new threats that never existed before in natural environments and dealt with classical natural risks by lowering their likelihood, impact, or frequency (e.g. watergates to diminish the risk of flooding). Against this shift human risk perception has not yet been adapted accordingly [Sch08]. Thousands of years ago these predispositions were essential for quick decision making in order to survive in hostile habitats – e.g. in case of a predator sighting either by fleeing and being chased, by apparent death, or by pre-emptive attack. Thus, leaving human behaviour nowadays with evolutionary flaws as a challenge for establishing security-aware organisational cultures.

Prior analyses and research in the area of security awareness were conducted by the SANS Institute on "Developing a Security-Awareness Culture" [Gar04], Paulsen & Coulson for the importance of *Business Intelligence (BI)* tools and measurements [PC11], and Da Veiga & Eloff for including security awareness in their "Information Security Governance Framework" [VE07]. Schlienger and Teufel discovered that with increased awareness a good information security culture can be established [ST03].

Most of the research found with focus on security-aware organisational cultures leaves factors like human nature and an employee's personality out of scope. It is the intention of this extended abstract to provide a more holistic view on how employees may threaten or support organisational security. The interdisciplinary nature of this topic makes it difficult: behavioural economics, psychology of decision making, psychology of risk, and neuroscience are all involved research actors [Sch08]. Furthermore, when including organisational culture one has to deal with cultural sciences, corporate psychology, and even evolutionary biology, too.

Hofstede developed a model for the uniqueness in human mental programming [Hof01] in which he distinguished three different levels: personality, culture, and human nature (Figure 1). The unique human mind is built upon the assumption of a universal human behaviour which is refined by learned cultural values as well as norms and finally formed by its individual personality.

Using Hofstede's fundamental model can assist in addressing proper approaches per level. E.g. understanding the role in and the identification of an employee with his or her organisational culture leads to more effective measures in changing cultural norms, in modifying the employee training, or in improving organisational policies more comprehensively. It is crucial to examine all three levels which can also be targeted by an attacker.

To approach the security awareness of an organisation I will focus in the following sections on each level of human behaviour whether found in universal human nature (2), cultural norms (3), or personality (4). Thereby it is important to mention, that in each section characteristics or factors exist which sometimes correlate or influence others in the same or in a different section. For instance, some personality traits are influenced by the cultural background: "Extraversion and Agreeableness [...] appear to be more sensitive to cultural context" [Rol02].

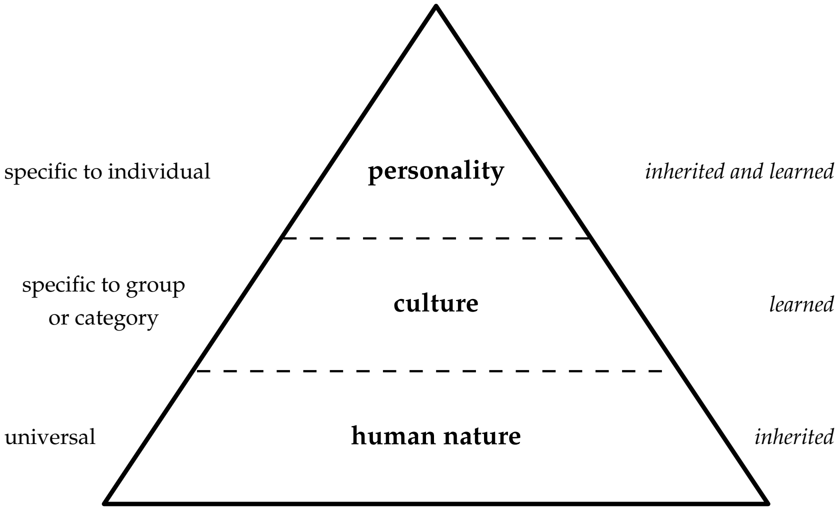

Figure 1: Three levels of uniqueness in human mental programming [Hof01]

## 2 Universal Human Behaviour

Security awareness in terms of universal human behaviour means to first understand and identify common vulnerablities in human behaviour in order to provide later analytic approaches for social attack discovery, effective training, comprehensible security policies, and even reactive and proactive countermeasures initiated by employees. Understanding these key characteristics based on evolution could lead to the development of a more sustainable awareness training because typically human risk awareness declines over time (relative to factors like incident frequency, impact, self-inflicted risk etc.) and therefore human nature tends to underestimate some of the risks [Sch08].

Preventing human flaws in risk perception by awareness training is a demanding undertaking. Nevertheless, this seems to be a general task applicable to most of the employees.

However, it is important that employees are active participants thereby consciously accepting training procedures and refining them.

Cialdini proposed in his seminal work [Cia07] six atomic key principles of influence, viz. reciprocity, commitment and consistency, social proof, authority, liking, and scarcity. Using these principles helps to understand feasible vectors of *SE* attacks and can lead to a more effective security aware environment and training. The challenge arises in mapping and assessing Cialdini's principles with respect to *SE* in general. Some principles seem more present like "authority" used for seducing employees to become an inside threat. An attacker can use "scarcity" to lure an employee into clicking on a link or attachment in an e-mail by offering a rare opportunity which needs immediate action to benefit from.

# 3 National and Organisational Cultural Classifications

The social environment and the socialisation of an individual has a big impact on how events are perceived and interpreted. Every individual's risk assessment contains its immanent social predispositions showing that one has to investigate social and cultural values and norms. Dawkins wrote in "The Selfish Gene" [Daw06, p. 99]: "Human customs and tribal rituals commonly give great emphasis to kinship; ancestor worship is widespread, family obligations and loyalties dominate much of life." And, as mentioned in the introduction, Rolland observed that two of the five personality traits discussed later in section 4 are sensitive to the cultural context [Rol02].

In comparison to the universal human behaviour social interaction is defined and passed on per specific social group with a sense of collective identity, therefore containing similar characteristics we can use as identification. Hofstede's cultural level of mental programming [Hof01] is explicitly defined by learned norms for a group or category and not built on a genetic or inherited ground.

In order to start and analyse possible research areas distinguishing between organisational culture and national culture seems promising – even if the word "nation" does not equal every cultural group. Although a direct correlation of cultures and security awareness seems difficult, their impact on human behaviour in security issues should not be disregarded. Cultural sciences are one provider of reliable reasearch results. Combining the research results of organisational and national cultures can provide us with a more holistic cultural view.

## 3.1 Organisational Culture

The analysis of the incident of sensitive data loss in transit between *HM Revenue and Customs (HMRC)* and *National Audit Office (NAO)* in the UK showed that cultural differences not only exist between organisations. Even in big institutions multiple cultural groups can be found where "different subcultural approaches to requesting and granting authorisation for data transfer" [PCK11] create security incidents. Thus, research on organisational cultures should include the examination of subcultures regarding their differences in security-related aspects, e.g. what one subculture understands as behaving compliant to security policies can vary from another one completely. This applies to security-aware behaviour as well. Organisational subcultures can be addressed by the (occupational) grouping of personalities of employees (see section 4).

Hofstede defined an organisational culture as "the collective programming of the mind that distinguishes the members of one organisation from others" [Hof13b]. Bate [Bat97] did extensive research on classifying corporate cultures and approaches to change them as well as Schreyögg [Sch99] describing key elements of both on which I based my diploma thesis [Üb02] starting to examine how different cultural characteristics could support corporate security. Schreyögg examined the key elements of corporate cultures, the rate of identification with it (definitions of strong and weak cultures) and their general functional and dysfunctional effects. Schreyögg [Sch99] proposed his six main characteristics of organisational cultures: implicit, collective, conceptional, emotional, historic, and interactive. Hofstede and Waisfisz [Hof13b] applied their dimensional approach to organisational cultures consisting of "six autonomous dimensions (variables) and two semi-autonomous dimensions" (cf. 3.2 National Cultures). Schein's three levels of a culture describes the "degree to which the cultural phenomenon is visible to the observer" to "differentiate the levels at which [culture] manifests itself" [Sch04, p. 25]. That includes how cultural characteristics are visible, noticed consciously, or interpreted.

None of the above mentioned cultural approaches focuses on organisational security or security awareness in particular, but are often used as a fundament on top of which security research is conducted. For example, Schlienger and Teufel present a way to create, change, and maintain an Information Security Culture [ST03] based on Schein's and Schreyögg's approaches. They conclude that increased awareness creates and supports a good security culture.

### 3.2 National Cultures

Hofstede's recent research demonstrates the ability to distinguish between cultural dimensions in national context where "organisational cultures differ mainly at the level of practices. These are more superficial and more easily learned and unlearned than values forming the core of national cultures." [Hof13b]. Widening the cultural view from organisational to national characteristics will give us a better understanding of how culture influences and shapes security awareness. The national culture as a more static society and the more dynamic organisational culture could complement one another nicely.

In his 5-D model Hofstede defined and put numbers on the five cultural dimensions per country, i.e. power distance, individualism, masculinity, uncertainty avoidance, and long term orientation [Hof13a]. To which extent these dimensions interact with security awareness needs to be examined.

**Power Distance (*PDI*)** is defined as the expectation and acceptance of unequally distributed power among members of institutions and organisations in a country.

**Individualism vs. Collectivism (*IDV*)** reflects “the degree of interdependence a society maintains among its members.”

**Masculinity vs. Femininity (*MAS*)** dimension describes the motivation of people what they think is important to achieve. Wanting to be the best is “masculine”, liking what you do defined as “feminine”.

**Uncertainty Avoidance (*UAI*)** specifies whether members of a culture experience “ambiguous or unknown situations” as a threat that needs to be avoided.

**Long-Term vs. Short-Term Orientation (*LTO*)** pictures the degree a society has towards a future-oriented or short-term perspective.

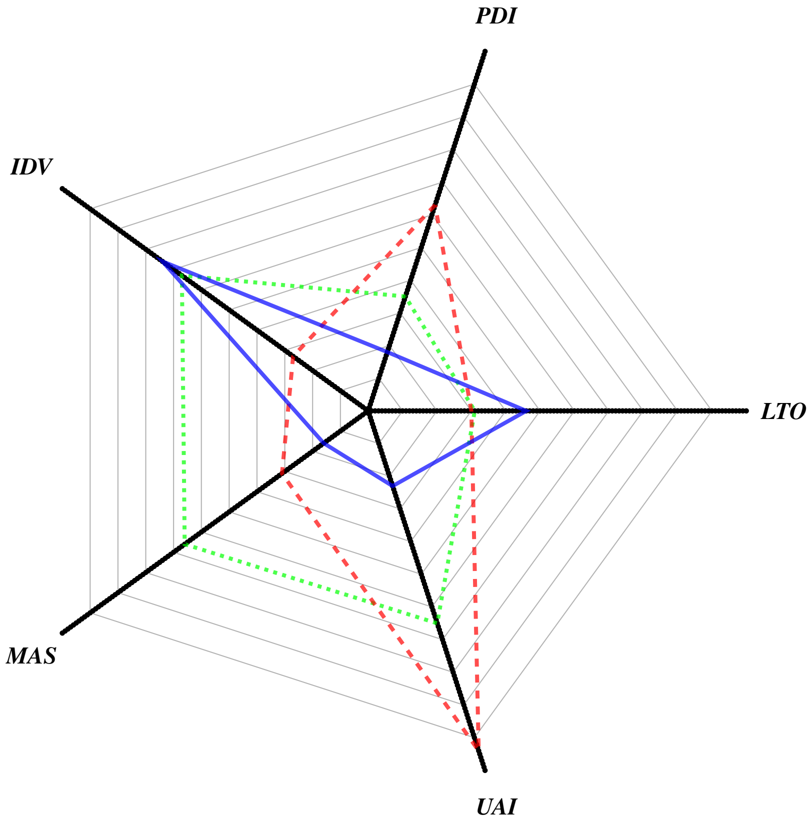

Figure 2: Example of five dimensions of national cultures [Hof13a]
Comparison of Denmark [blue line], Germany [green dotted], and Portugal [red dashed]
(every 10th grid line drawn)

Hofstede et. al. presented the findings of their analysis in block charts for comparision of different national cultural values. The spiderweb visualisation I used in Figure 2 seems a better way to contrast specific characteristics to me. If further analysis of these dimensions provides us with a meaningful orientation whether a high or low value should be prefered for a security-aware culture, the axes could be aligned (scale and value per dimension) in such a way that the enclosed region per nation gives us a sense on how the national culture impacts security awareness.

As national cultures tend to stay out of an organisation's influence they offer a cultural frame in which organisational cultures flourish. Norms and behaviours typical to national cultures should be taken into account when analysing, evaluating, or changing organisational cultures.

### 3.2.1 Comparison of Denmark, Germany, and Portugal

For example, the exceptional high value (104) of uncertainty avoidance for Portuguese culture shows that there exists an "emotional need for rules", that security plays a big role, and "innovation may be resisted" (UAI description of Portugal in [Hof13a]). Hence, it can offer an awareness for anomal behaviour, but also can create a challenge for changing once established norms and policies towards organisational security. Denmark takes on an opposite role regarding uncertainty avoidance with a value of 23 (UAI description of Denmark in [Hof13a]) where misaligned or inconsistent definitions of security policies can be assumed less important. Whereas Denmark's higher value of 46 in long term orientation could result in a more sustainable path for a security-aware culture.

Germany differs in a very masculine society (66) from Portugal (31) and Denmark (16), i.e. one's indivual performance is higher valued than an achievement of their social group. The personal status is reflected in a more competitive, materialistic way and "a lot of self-esteem [is drawn] from their tasks" (MAS description of Germany in [Hof13a]). This could indicate that the identification with their work is more intense, but competing employees within an organisation could counteract the team spirit (cf. Germany's high value for individualism). On the other hand rewarding individuals on good security-aware behaviour could be an incentive.

## 4 Personality of Employees

Despite the sensitivity of dealing with an employee's personality because of conflicts in labor legislation and human rights, aggregation in pseudonymic categories could be a way forward depending on which characteristics aggregation is performed. This intentionally excludes the analysis of an individual's psychological imprints.

A widely used approach to describe personality traits is bases upon the *Five Factor Model (FFM)*, also known as the "Big Five" [BM91]. The *FFM* consist of "Openness", "Conscientiousness", "Extraversion", "Agreeableness", and "Neuroticism/Emotional Stability" as key dimensions as depicted in Figure 3. Correlating the results of *SE* attacks with these Big Five factors can give us a comprehensive view on vulnerabilities in human behaviour originating from one's personality and support a sustainable education process.

For instance, security-aware employees with higher level of conscientiousness can tend to comply better with (evolving) security policies or changing organisational security cultures because of a distinct self-discipline and a stronger occupational identification. Whereas a high level of “Agreeableness” can lead to helping an attacker getting access to a restricted area or system because of the compassion shown even to strangers.

Schlienger’s and Teufel’s research showed [ST03] how grouping of employees can be performed based on an analysis of Orange Switzerland. On one hand their “Segmentation of Organizational Members” consists of distinguishing between functions (IT vs. business) and positions (employee vs. manager) which revealed statistical significant differences. On the other hand they applied a statistical cluster analysis in order to group employees with similar attributes gathered by the same survey. This led to four clusters: “I’m happy” (44%), “Danger comes from outside” (19%), “Careless people” (4%), and “I’m unhappy” (32%).

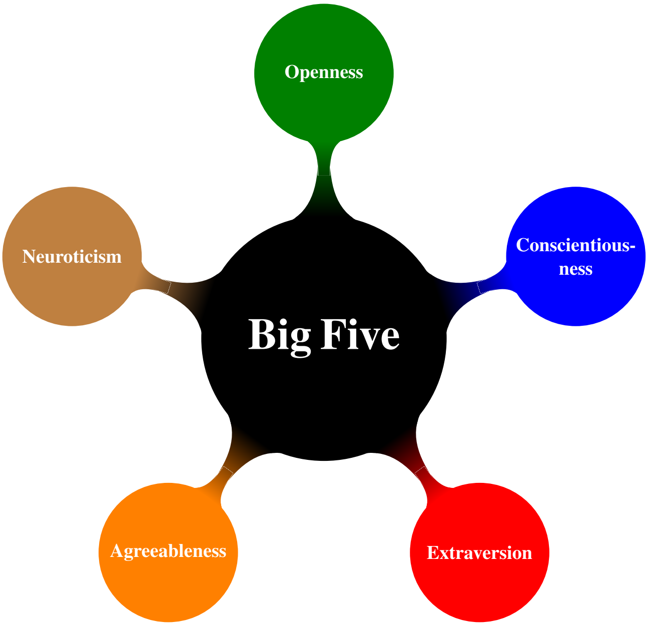

Figure 3: *FFM* personality traits (OCEAN) [BM91]

Hossiep and Paschen [HP04] were able to describe an employee’s personality traits by their type of occupation. They call it *Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP)*, a German personality inventory for organisational applications. *BIP* is based on personality tests and focuses on exploring occupational personality traits containing the main charts: occupational orientation, work habits, interpersonal skills, and mental constitution [HP04]. The most recent version BIP-FV Revision VI includes new aspects like competitive orientation, analysis orientation, and enthusiasm [Hos13]. A study revealed the concurrent validity of the *BIP* and the personality test “NEO-PI-R” based on the *FFM* both of which “contributed significantly to the explanation of objective and subjective indicators of career success” [HSS06]. If this applies for security awareness as well it needs to be analysed in order to have a wider variety of personality tests and available empirical data at hand.

The data provided by *BIP* and similar databases could assist in detecting unaligned or misunderstood security policies, lack of awareness against *SE* attacks, wrong training or communication practices. To which extent these charactistics identify vulnerable human behaviour needs further investigation.

## 5 Outlook

First of all Hofstede’s model of mental programming gives us an overview of how an individual’s mind could be reached. The interdisciplinary nature of this undertaking becomes a challenge in all research areas, either by modelling human behaviour or by maintaining a regularly updated collection of empirical data. Furthermore, all these disciplines have to combine their efforts to address human behaviour in order to discover their influence on security awareness.

An organisation can manage its own organisational culture actively with a top-down or indirectly via a bottom-up strategy to achieve security policy compliance, e.g. via security awareness. In case of a bottom-up strategy management has to trust in the decision making of their employees which could result in a shift of emphasis in the organisational culture. Because an organisation cannot bring leverage to bear on the surrounding human and cultural factors directly, dealing with its own organisational culture presents a feasible starting point. Which management strategy could be promising needs further analysis.

In case of influential characteristics to the *FFM* dimensions experiential factors, gender, and age need to be added for examination beside the discussed organisational and national cultures [PJBC09, p. 6]. Both dimensions of human factors in information security (namely knowledge and human co-operated behaviour [VNvS05]) should be targeted for suitable measures in order to establish a security-aware organisational culture.

Before management will be able to determine which educational (in relation to knowledge) and cultural change procedures (addressing co-operated behaviour) should be launched, a profound analysis of the status quo of security practices according to the security policies in place has to be conducted. With respect to employee’s behaviour an assessment of all three levels of Hofstede’s model requires attention. For instance, Hasle et al. provide a concept and metrics for the measurement of resistance against *SE* attacks [HKKS05].

For the educational part research towards an *Outcome-Based Education (OBE)* was done by Niekerk [VNvS05]. Schlienger and Teufel introduced the interesting aspect of applying the theory of internal marketing for defining socio-cultural measures in their “Security Awareness and Training Program” to “sell information security aware behaviour to [the] employees” [ST03]. According to McBride et al. [MCW12] cybersecurity training should be adapted properly for each unique audience. This idea can be included in an educational concept for a security-aware organisational culture which is the starting point for an information security culture [ST03].

All in all, a sustainable and reoccurring process for generating a security-aware organisational culture can become the first step in a socio-technical immunisation program if employees are identified as organisational assets.

## 6 Acknowledgement

Part of the research leading to these results has received funding from the European Commission's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 318003 (TRE$_S$PASS).

## 7 Nomenclature

| | |
|---|---|
| ***BYOD*** | Bring Your Own Device |
| ***BI*** | Business Intelligence |
| ***BIP*** | Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung |
| ***FFM*** | Five Factor Model |
| ***HMRC*** | HM Revenue and Customs |
| ***IDV*** | Individualism in Hofstede's 5-D model |
| ***LTO*** | Long-Term Orientation in Hofstede's 5-D model |
| ***MAS*** | Masculinity in Hofstede's 5-D model |
| ***NAO*** | National Audit Office |
| ***OBE*** | Outcome-Based Education |
| ***PDI*** | Power Distance in Hofstede's 5-D model |
| ***SE*** | Social Engineering |
| ***UAI*** | Uncertainty Avoidance in Hofstede's 5-D model |

## References

[Bat97] Paul Bate. *Cultural Change – Strategien zur Änderung der Unternehmenskultur.* Gerling Akademie Verlag, 1997.

[BM91] Murray R. Barrick and Micheal K. Mount. The Big Five Personality Dimensions and Job Performance: A Meta-Analysis. *Personnel Psychology*, 44(1):1–26, 1991.

[Cia07] Robert B. Cialdini. *Influence: The Psychology of Persuasion*. HarperCollins, 2007.

[Daw06] Richard Dawkins. *The selfish gene*. Oxford University Press, 2006.

[Gar04] Chris Garrett. Developing a Security-Awareness Culture – Improving Security Decision Making. *SANS Institute InfoSec Reading Room*, 2004.

[HKKS05] Hågen Hasle, Yngve Kristiansen, Ketil Kintel, and Einar Snekkenes. Measuring Resistance to Social Engineering. In *Information Security Practice and Experience*, pages 132–143. Springer, 2005.

[Hof01] Geert Hofstede. *Lokales Denken, globales Handeln*. Beck–Wirtschaftsberater im dtv, 2. edition, 2001.

[Hof13a] Hofstede Center. National Cultural Dimensions. 2013. `http://geert-hofstede.com/national-culture.html` visited on May 07, 2013.

[Hof13b] Hofstede Center. Organisational Culture & Change Management. 2013. `http://geert-hofstede.com/organisational-culture.html` visited on April 30, 2013.

[Hos13] Hossiep, Rüdiger et al. Bochumer Inventar zur berufsbezogenen Persönlichkeitsbeschreibung (BIP). 2013. `http://www.testentwicklung.de/testverfahren/BIP/index.html.de` visited on May 07, 2013.

[HP04] R. Hossiep and M. Paschen. Rezension der 2. Auflage des Bochumer Inventars zur berufsbezogenen Persönlichkeitsbeschreibung (BIP). *Zeitschrift für Arbeits-und Organisationspsychologie A&O*, 48(2):79–86, 2004. `http://www.psycontent.com/content/f95u4k767h07825r/`.

[HSS06] Ute R Hülsheger, Elke Specht, and Frank M Spinath. Validität des BIP und des NEO-PI-R. *Zeitschrift für Arbeits-und Organisationspsychologie A&O*, 50(3):135–147, 2006.

[MCW12] Maranda McBride, Lemuria Carter, and Merrill Warkentin. One Size Doesn't Fit All: Cybersecurity Training Should Be Customized. Technical report, Institute for Homeland Security Solutions, 2012. `http://sites.duke.edu/ihss/files/2011/12/CyberSecurity_2page-summary_mcbride-2012.pdf`.

[PC11] Celia Paulsen and Tony Coulson. Beyond Awareness: Using Business Intelligence to Create a Culture of Information Security. *Communications of the IIMA*, 11(3):35–54, 2011. Communications of the IIMA 2011 Volume 11 Issue 3.

[PCK11] Wolter Pieters and Lizzie Coles-Kemp. Reducing normative conflicts in information security. In Sean Peisert, Richard Ford, Carrie Gates, and Cormac Herley, editors, *NSPW*, pages 11–24. ACM, 2011. `http://www.nspw.org/papers/2011/nspw2011-pieters.pdf`.

[PJBC09] James L Parrish Jr, Janet L Bailey, and James F Courtney. A Personality Based Model for Determining Susceptibility to Phishing Attacks. *Little Rock: University of Arkansas*, 2009. `http://www.swdsi.org/swdsi2009/Papers/9J05.pdf`.

[Rol02] Jean-Pierre Rolland. The Cross-Cultural Generalizability of the Five-Factor Model of Personality. In Robert R. McCrae and Jüri Allik, editors, *The Five-Factor Model of Personality Across Cultures*, International and Cultural Psychology Series, pages 7–28. Springer US, 2002.

[Sch99] Georg Schreyögg. *Organisation – Grundlagen moderner Organisationsgestaltung*. Gabler Verlag, 3. edition, 1999.

[Sch04] Edgar H. Schein. *Organizational Culture and Leadership*. Jossey-Bass, 3. edition, 2004.

[Sch08] Bruce Schneier. The Psychology of Security. In Serge Vaudenay, editor, *AFRICACRYPT*, volume 5023 of *Lecture Notes in Computer Science*, pages 50–79. Springer, 2008. https://www.schneier.com/paper-psychology-of-security.pdf.

[ST03] Thomas Schlienger and Stephanie Teufel. Information Security Culture – from Analysis to Change. *South African Computer Journal*, pages 46–52, 2003.

[VE07] A. Da Veiga and J. H. P. Eloff. An Information Security Governance Framework. *Information Systems Management*, 24(4):361–372, 2007. http://www.tandfonline.com/doi/pdf/10.1080/10580530701586136.

[VNvS05] Johan Van Niekerk and Rossouw von Solms. An holistic framework for the fostering of an information security sub-culture in organizations. *Information Security South Africa (ISSA), Johannesburg, South Africa*, 2005. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.102.6622&rep=rep1&type=pdf.

[Üb02] Sven Übelacker. IT-Sicherheit, Unternehmenskulturen und wirtschaftsbedrohende Kriminalität. diploma thesis, University of Ulm, 2002.