CLTRe
a KnowBe4 company

Research paper by CLTRe

The seven dimensions of security culture

By: Aimee Laycock, Gregor Petric and Kai Roer

https://www.knowbe4.com/security-culture

Content

About the authors

Experienced security culture experts co-author this paper. The authors are influential voices in the academic and professional space, driving both scientific research and industry discourse.

Aimee Laycock

COO

Aimee has a BSc (Hons) in business economics, and is a co-founder and the COO of CLTRe, where she is managing the marketing, outreach and customer success. She is a key part of turning the science of CLTRe into read-worthy publications.

Gregor Petrič

Chief Science Officer

Gregor is an associate professor at the University of Ljubljana, where he chairs the Center for Methodology and Informatics. He co-founded CLTRe, and his research lays the groundwork for the security culture metrics instrument and methodologies created by CLTRe.

Kai Roer

CEO

Kai is a security veteran and serial entrepreneur who co-founded CLTRe. He is passionate about providing evidence over opinions and has been instrumental to the creation of the CLTRe Toolkit - from the concept and architecture design through to business development.

Executive summary

Information security risks and threats, such as viruses, spyware, ransomware and phishing, are an increasingly significant issue. IBM reports that as many as one in four companies[1] are affected by cyber-crime. In nine out of ten incidents[2], the criminals get in using social engineering, often by using stolen credentials gained through phishing or by planting malware in email attachments.

Weak information security culture has led to unwanted exposures of personal sensitive information of billions of individuals worldwide[3], and information security attacks are a major concern. In the US, a typical data breach now costs a company $7.91M[4]. Not surprising then, that as many as 60 percent of hacked small and medium-sized businesses reportedly go out of business after six months[5].

As a result, we are seeing security culture rise as a recognised need in organizations, and driving this change in approach has been the acknowledgement within organizations that[6]:

a) Technical cyber security measures need to operate in harmony with other business processes.

b) Employees should not be put in a conflicting situation, where they forced to choose between complying with security policies or doing their job.

c) Cyber threat awareness-raising campaigns are not, in themselves, affording sufficient protection against ever-evolving cyber-attacks.

d) How an organization behaves is dependent on the shared beliefs, values and actions of its employees towards information security.

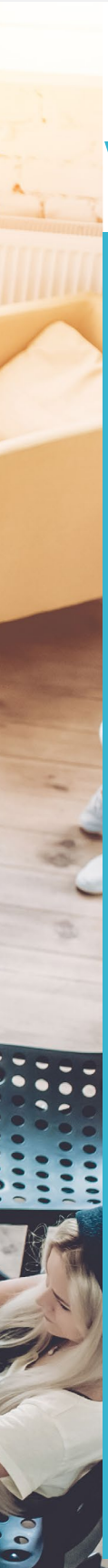
e) Rather than view employees as the weakest link in cyber security chains, they should instead be viewed as an important line of defence (a human firewall) against cyber-attacks.

There have been considerable efforts from information security industry and experts to make countermeasures and solutions available to detect, prevent, and minimise losses from information security attacks. However, it is important that organizations

understand that developing a strong security culture is an important and effective strategy to improve risk management. Not a one-off activity, security culture is an ongoing process that needs to be continuously nurtured and incorporated into the wider organizational culture.

In our research, we have developed and investigated the following seven key dimensions of security culture; employee attitudes to security and policies, behaviors, cognitive processes surrounding security, quality of communication, compliance to security policies, organizational unwritten rules or norms, and individual responsibilities.

Information about these dimensions is vital when it comes to improving security culture, and thus reducing risk in the organization. This text builds on CLTRe's model for measuring security culture and provides a comprehensive resource for practitioners seeking a deeper understanding of the dimensions that comprise security culture. Knowing what these dimensions are, how they relate to security, and how they can be positively influenced, will provide practitioners with the tools and practical advice needed to start building and improving security culture in organizations.



What is security culture?

Security culture depicts the human-related security elements in organizational settings, and is defined by the Security Culture Framework as "the ideas, customs, and social behavior of a particular people or society [i.e. employees in an organization] that allow them to be free from danger or threats"[7].

This definition is useful in order for practitioners to understand the wider concept of security culture. However, when we want to measure a phenomenon, a more detailed definition is often required. In this document we describe the 7 dimensions that CLTRe and our research partners have identified as the core elements that need to be measured in order to describe security culture accurately.

In order to be able to improve a security culture (e.g. to make it stronger or more positive), we need to know what we mean by the concept of security culture, i.e. what human or organizational aspects are we referring to. Only then will we know what makes a security culture strong or positive in the first place. Once it is defined, we can measure it. Using the results, we discover what mechanisms can be used to influence security culture, and the extent of their impact.

> *The ideas, customs and social behavior of a particular people or society that allow them to be free from danger or threats.*
> *– The Security Culture Framework*

The following text elaborates on our model for measuring and managing security culture. This model is comprised of seven dimensions and includes human-aspects of security that existing models often omit, such as organization communication processes, social roles and a more comprehensive understanding of norms, attitudes and cognitive processes. Much care has been taken to explain what each of the dimensions are, where they come from, why they matter, and how they fit into the overall model for measuring security culture.

A metric is a standard of measurement

Imagine the following conversation between a CISO and his CEO. The CISO reports, "We have positive security culture in our organization." The CEO responds, "Great, but what does that mean? How do you know?" Pushing further, he asks, "Does this mean we are better than X, Y or Z? How does this impact our risk?"

The challenge for the CISO is that unless she has a way to measure security culture, she cannot answer his questions. She may have opinions to offer CEO, or reasons, but it will be very difficult for her to back those up without strong empirical evidence.

To provide that evidence, a security culture metric is needed. A metric is a standard of measurement. Because it is a standard, everyone has a clear understanding of what it is, what it measures, and what it is not measuring. Despite the fact that the words mass and weight are commonly used interchangeably, everyone understands that a kilogram measures mass; not weight.

Security culture metrics serve the purpose of measuring security culture, they are not measuring awareness training completion rates or phishing assessments. Security culture metrics measure the sentiments towards security in an organization - the psychological and social aspects that drive individual and social behavior.

By using a standardized metric to measure security culture in the organization, the CISO can provide good answers for the CEO. She can create a baseline measurement for comparison to consecutive measurements, and even track progress against industry benchmarks. Security culture metrics provide a way to demonstrate how the heart and minds of an organization are changing, and reveal how strong the bricks and mortar of your human firewall is.

CLTRe provides standalone, unbiased and independent security culture metrics. With our solution, organizations can take an evidence-first approach to measure, improve and document the changes in their security culture – knowing that the effects can be compared in a meaningful way.

In security, there are three interrelated pillars that organizations need to build and maintain: people, tools, and processes. The people-aspect, and in particular the

Modeling security culture

understanding of how people use tools and processes, is little understood.

There has been an increase in the scientific and professional literature exploring this area in recent years, however a critical observation is that these studies mainly focus on psychological factors, while neglecting sociological and organizational factors.

Some academic research in this area includes DaVeiga and Martins' Information Security Culture Assessment Model and Rocha Flores and Ekstedt's Information Security Culture Model. The Security Culture Toolkit is more complete, because in addition to addressing the sociological, psychological and anthropological perspectives, our model includes human-aspects of security that are often omitted, such as organization communication processes, social roles and a more comprehensive understanding of norms, attitudes and cognitive processes.

A lot of research is hindered by the fact that it only collects data from IT administrators or top-level managers and there is hardly any representation from the end-user community[8]. Because we measure the security culture of every employee in an organization (and perform analysis on how each of the dimensions of security culture influences end-user behavior in different organizational contexts), CLTRe plays an important role in putting empirical research of end-user behaviors, identification of their factors, and security culture in general at a higher level.

Since employees are often not willing to admit to committing unethical behaviors, it is important to identify and use the appropriate research methodologies to capture these phenomena in a way that reflects reality. It is also worth noting that while organizational monitoring techniques can be used to collect data on employee behaviors, in practice such process is extremely costly and are not always possible. For instance, it is not practical to monitor behaviors such as writing down passwords or sharing passwords with friends[9].

Our security culture model is an important element of a wider Security Culture Framework. The model consists of seven dimensions: *attitudes, behaviors, cognition, communication, compliance, norms, and responsibilities*.

These seven dimensions were identified, tested and validated by the CLTRe Research team (headed by our Chief Science Officer, Dr. Gregor Petrič) in conjunction with our research partners including the Research Center for Methodology and Informatics at the University of Ljubljana.

Our measurement items assess a variability of different practices and activities of employees. The items are formed in a neutral manner so that even self-reported assessments provide a good measurement of culture.

The 7 dimensions of security culture

Attitudes

The feelings and beliefs that employees have toward the security protocols and issues.

The seven dimensions used by CLTRe to model security culture pertain to the human factors (i.e. the core human-related elements) that have a direct or indirect impact on the security of the organization.

Each dimension is separately observed, measured and understood on a continuum from low risk to high risk. This is informative for organizations, especially when the dimensions are seen together. Combining the dimensions creates an accurate estimate of an organization's security culture and allows an organization to fully and deeply understand the human risks involved and make reliable predictions.

While the dimensions are interconnected in a complex web of causes and effects, empirical research shows that each organization demonstrates a specific system of interconnections among dimensions. The dimensions are correlated to each other, although some more strongly than others. Like cogs in a machine, each dimension is crucial for the machine to function properly.

Data obtained by measuring each dimension of security culture allows for direct comparisons of the extent to which each dimension of security culture is developed; or looking from another perspective, these metrics reveal which dimensions are most problematic and risky. Moreover, the Security Culture Toolkit allows highly reliable evidence-based decision making as the data allows its users to identify the main causal mechanisms in the organization.

To give a couple of examples, the data can show that in certain organizations end-user behavior is primarily dependent on the quality of communication in the organization, clearly calling for actions on the level of organizational communication processes. In another organization, the data may show that compliance is problematic because of lack of clear dissemination practices and an indifferent attitude of department leaders to security policies, calling for interventions at that level.

For each organization and even department, we can compare the strength of influence of knowledge and awareness on employee behavior with the strength of influence of norms, attitudes, communication processes, roles and compliance and make predictions on this basis.

The following chapters seek to provide a deeper understanding of each dimension, and why these seven dimensions are specifically used to measure security culture.

Behaviors

The actions and activities of employees that have direct or indirect impact on the security of the organization.

Cognition

The employees' understanding, knowledge and awareness of security issues and activities.

Communication

The quality of communication channels to discuss security-related events, promote sense of belonging, and provide support for security issues and incident reporting.

Compliance

The knowledge of written security policies and the extent that employees follow them.

Norms

The knowledge of and adherence to unwritten rules of conduct in the organization, i.e. how security-related behaviors are perceived by employees as normal and accepted or unusual and unaccepted.

Responsibilities

How employees perceive their role as a critical factor in sustaining or endangering the security of the organization.

The feelings and beliefs that employees have toward the security protocols and issues.

Attitudes

The feelings and beliefs that employees have toward the security protocols and issues.

Commonly expressed in terms such as prefer, like, dislike, hate, and love, attitudes involve a preference for or against something. When we express our attitudes, we are expressing the relationship (either positive or negative) between the self and an attitude object[10, 11]. For example

"I like my security badge,"

"I hate changing my password," or

"I love my job."

Because attitudes are evaluations, they can be assessed using any of the normal measuring techniques used by social psychologists[12], such as self-report measures like questionnaires. Measuring attitudes in general has a long history since first attempts were published by Thurstone in 1929.

Social psychology has discovered that our attitudes are made up of cognitive, affective, and behavioral components. Stangor provides the following illustrative example in his book, Principles of Social Psychology, "consider an environmentalist's attitude toward recycling, which is probably very positive:

In terms of affect: They feel happy when they recycle.

In terms of behavior: They regularly recycle their bottles and cans.

In terms of cognition: They believe recycling is the responsible thing to do."

He explains that although some attitudes are more likely to be based on feelings, some are more likely to be based on behaviors, and some are more likely to be based on beliefs[13].

Learned mostly through direct and indirect experiences with the attitude object[14], an attitude is likely to be stronger if there is direct experience[15]. Psychology claims that while attitudes are enduring, they can also change. Various theories describe how attitudes can change, from learning theory to persuasion theory. Augoustinos et al. (2006) point out that attitudes need to be 'activated' (p.116) in an individual.

This has significance for information security research as quite often participants may not have activated attitudes towards information security or the protection of information. They are more likely to have activated attitudes if they have direct experience of the topic (either in their organizational role or personal experience of an information security incident). Whilst psychology views that most attitudes are determined by affect, behavior, and cognition, it excludes the role of social context.

Interestingly behavioral research in information security until recently disregarded an important finding from classical social psychology that not only can attitudes impact behavior, but behaviors also influence attitudes. If we engage in a behavior, and particularly one that we had not expected that we would have, our thoughts and feelings toward that behavior are likely to change[17]. This pertains to the principle of attitude consistency

and is coming from the process of self-perception, when we use our own behavior as a guide to help us determine our own thoughts and feelings[18].

Attitudes are the subject of controversy. As mentioned, psychology studies tend to explore how behavior influences attitudes. Conversely, behavioral security research tends to focus on how employee attitudes directly influence information security behaviors. This focus of research on the influence of attitudes on behavior is not surprising as it is one of the most commonly applied socio-psychological theories in this field; the Theory of Planned Behavior.

The Theory of Planned Behavior (later upgraded into the Theory of Reasoned Action[19]) exposes attitudes as an important antecedent of behavioral intent. For example, research[20] points out that employees are aware that a password breach can have serious consequences for them and for the organization, but their attitudes toward following security policy remained negative or indifferent, resulting in continued risky behavior. Such discrepancy between knowledge, attitudes and behaviors is well known in social psychology.

Cognitive dissonance is a concept that describes a tension between individual beliefs and activities, e.g. "I shouldn't smoke, because it is bad for my health. I nevertheless smoke". People have tendency to resolve such tense state of mind by rather changing attitude ("My grandfather smoked and lived until he was 90 years old, so it's not so bad") than behavior (I stop smoking). Similar situations are noticed in the security field, when employees instead of practicing conscious risk-averse behavior (i.e. use stronger passwords), change attitudes toward security behavior ("Why would hackers attack me if I'm just an ordinary employee").

Behavioral security research shows that such attitudes are an important predictor of end-user behaviors and can at the same time be influenced by various mechanisms[21]. It has been empirically demonstrated that different training methods also change our attitude towards certain issues[22]. However, behavioral security research is not yet conclusive regarding the main predictors of attitudes and also about how exactly and with what strength attitudes impact security behaviors.

Nevertheless, exploring employee attitudes towards cyber security provides an important metric to help target awareness in a more proactive way[23]. Hadlington (2018) observed that negative attitudes are manifested by employees who see reporting cyber incidents as a waste of time.

Attitudes of employees toward organizational security policy, toward conscious use of IT devices and toward organizational security in general are an important part of security culture. Information security awareness of risks influences the attitude towards behavior in the users[24]. Ifinedo (2014) showed that attitude, subjective norms, and perceived behavioral control influence users' intention to comply with information security organization policies.

Measuring attitudes of employees (on all levels of company) toward information security policy and security-related activities is immensely important for an organization to get an estimate of overall sentiment toward security issues in an organization.

Tips for positively influencing attitudes towards security in the organization

An attitude is likely to be stronger if there is direct experience. Attitudes can be changed by reinforcing positive norms and through effective communication. We recommend using techniques such as:

- ☐ Celebrating achievements. (See Norms.)
- ☐ Acknowledging concerns. (See Communication.)
- ☐ Involving other members of the organization in planning. (See Responsibilities.)
- ☐ Exemplifying behaviors by sharing examples of correct and desired behavior. (See Behaviors.)
- ☐ Empowering employees by providing adequate tools and processes. (See Compliance.)

The actions and activities of employees that have direct or indirect impact on the security of the organization.

Behaviors

The actions and activities of employees that have direct or indirect impact on the security of the organization.

Behaviors of employees when using information-communication devices are the most researched and theoretically discussed element of security culture and of behavioral information security research in general. Unsurprising as actions of employees are in the end those that are direct causes of security breaches and incidents[25]. Employees can execute activities of great threat to organizational assets[26]. Whether they act intentionally or unintentionally, in our industry, these employees are referred to as insider threats or insiders.

Empirical research on end-user security behaviors and factors influencing them is still in its infancy[27]. Research in general shows that there are different types of users, where a large number of them behave in a non-malicious way, but also have low technical knowledge related to password creation and sharing, which shows that password ''hygiene'' is generally poor[28].

Most users reuse the same password from site to site, and most users rely on the same patterns when making passwords[29]. A 2018 study of 6.1 million passwords[30], identified that the practice of using combinations of letters, numbers, and symbols that are adjacent to one another on the keyboard, like "qwerty" and "123456," is still alarmingly commonplace. However, behaviors also vary substantially across different organization types[31].

Other unintentional "misbehaviors" may include carelessly clicking on phishing links in emails and on websites, visiting non-work related websites using corporate computers, inadvertently posting confidential data onto unsecured servers or websites, or selecting a simple password. Another type of problematic end-user behavior in organizations recognised by information security behavioral research is "deviant behavior"[32]. Deviant behavior describes those actions which are intentional and are often labeled as sabotage, stealing, and industrial or political espionage.

Behaviors are generally very difficult to change, but not impossible. Information security behavioral research has adopted a number of theories from social psychology to find the key factors that influence behaviors. The most popular is the Theory of Planned Behavior, where behavior is a function of a person's attitude toward the behavior, the norms that people around the person have (i.e. social pressure), and the person's own feeling of control over their behavior (i.e. how easy it is for the person to perform one behavior)[33]. Another popular theory is Protection Motivation Theory[34], which delineates two main factors of behavior: Information security threat appraisal and self-efficacy. In addition, we can find further theories[35] that try to explain behavior change, but the field of behavioral information security research is at the moment not yet conclusive about the main factors.

A lot of research is hindered by the fact that it only collects data from IT administrators or top-level managers, resulting in low representation from the end-user community[36]. However, because we measure the security culture of every employee in an organization (and perform analysis on how each of the dimensions of security culture influences end user behavior in

different organizational contexts), CLTRe plays an important role in putting empirical research of end-user behaviors, identification of their factors, and security culture in general at a higher level.

Data obtained by measuring each dimension of security culture allows for direct comparisons of the influence of individual dimensions of security culture. Our studies show that end-user behavior is empirically dependent on the dimensions of security culture. We can compare the strength of the influence of knowledge and awareness on employee behavior with the influence of norms, attitudes, communication processes, roles/responsibilities and compliance and make predictions on this basis.

In particular, using predictive statistics we identified significant influences of perceptions of organizational norms on employee behavior. What is perceived as normal behavior in social settings has a strong influence on what is considered acceptable behavior in an organization and what is not, independent of what the rules or formal policies dictate.

Tips for positively influencing behaviors

Employee behavior is empirically dependent on the dimensions of security culture:

- ☐ Normal behavior in social settings has a strong influence on acceptable behavior in an organization. (See Norms.)
- ☐ Different training methods may change our behavior of certain issues. (See Attitudes.)
- ☐ Implement short communications that are easily available to the employee. (See Communication.)
- ☐ Identify processes that are important, and assess employees knowledge of their existence. (See Cognition.)
- ☐ Information security policies guide all employees on what behavior is expected and how to conform. (See Compliance.)

The employees' understanding, knowledge and awareness of security issues and activities.

Cognition

The employees' understanding, knowledge and awareness of security issues and activities.

It is argued that if a person is not aware of basic concepts of information security, he or she is more prone to information security threats than the others. Thus, knowledge is one of the key concepts in the research of human factor in information security, and it is a dominant component of information security awareness[37]. However, knowledge is a necessary but insufficient condition for employees to practice conscious careful behavior and to adhere to information security policies[38].

Empirical research shows practically non-existent correlations between knowledge and information security behavior[39], suggesting that employees who know more about security issues do not necessarily perform more secure end-user behaviors. This does not mean that knowledge is irrelevant in keeping organization safe. We just need to be aware that relation between knowledge and behavior is not direct and linear. Knowledge gained by employees can provide reliable insight into which processes are important to monitor and improve in order to strive for a change in employee behavior[40].

Although the field of behavioral information security focuses on the concept of awareness, traditional security education, training, and awareness approaches are often ineffective in preventing violations[41], so it is imperative that we explore other approaches to designing programs and how they communicate policies to better persuade employees to comply[42].

Knowledge Management Theory[43] defines knowledge as the contextual and high-value form of information and experience that positively affect decisions and actions[44]. Whereas, cognition pertains to the contextual information, awareness, and personal experience ready to be used for decisions and actions. It is this distinction that leads us to the conclusion that a focus on knowledge and awareness is not a comprehensive approach in understanding cognitive processes related to security. Instead we focus on the concept of cognition.

The concept of cognition generally refers to a range of mental processes relating to the acquisition, storage, manipulation, and retrieval of knowledge[45]. Research by Farooq & Vitanen (2015) suggests that there are three cognitive skills necessary for effective learning experience:

1) knowledge of facts, processes and concepts,

2) ability to apply the knowledge,

3) ability to reason[46].

These cognitive skills are developed through thought, experiences and senses[47]. Measuring the organization's cognition of security tells us what employees verifiably know or believe, what they understand of security-related issues and practices, as well as how they apply their knowledge. Our concept of cognition is therefore a combination of information, awareness and experience. We understand the acquisition of knowledge and understanding as parts of a wider set of cognitive processes, including but not limited to: awareness, action, emotions, memory, senses, thinking, planning, reasoning, and problem solving.

Assessments of employee cognition are important for organizations for various reasons. Foremost, knowledge is a necessary condition for other processes to unveil in order to have a secure organization. Knowledge and related cognitive processes are usually measured via self-reporting method, which gives good enough data, as it shows how confident users feel regarding a phenomenon[48].

We are interested in understanding and improving the process of acquiring knowledge and understanding of security-related issues. Information security awareness is important, but not a comprehensive approach in understanding cognitive processes related to security. We suggest that researchers and practitioners should look more broadly than the concept of security awareness and combine understanding processes of acquiring and using knowledge with other dimensions of security culture to get a comprehensive understanding of the role that knowledge plays in security of organization.

Higher levels of cognition help employees understand critical factors in improving security culture, such as how important their behavior is in sustaining or endangering the security of the organization, which can help build a sense of responsibility as well as support a sense of belonging and improve communication channels.

It is paramount that awareness trainings and other educational tools designed to build knowledge of security are tailored to the needs and learning styles of the individual. Tailoring education using target audiences improves the effectiveness of security culture programs, increases employee involvement and engagement, and improves cognition. The information gathered by security culture metrics can be used identify these needs and create target audiences.

Tips for positively influencing cognition

Whilst knowledge by itself is unlikely to have a direct impact on behavior, the cognitive processes required to acquire knowledge related to security have a direct and indirect influence on other dimensions that are significant to improving security culture:

- ☐ Establish clear expectations from the start. (See Norms and Compliance.)
- ☐ Share stories that advertise the security-related social norms and support a sense of belonging. (See Communication and Norms.)
- ☐ Emphasise the important role that each employee has is in sustaining the security of the organization. (See Responsibilities.)
- ☐ Ensure awareness trainings and other educational tools designed to build knowledge of security are tailored to the needs and learning styles of the individual.

The quality of communication channels to discuss security-related events, promote a sense of belonging, and provide support for security issues and incident reporting.

Communication

The quality of communication channels to discuss security-related events, promote a sense of belonging, and provide support for security issues and incident reporting.

Communication is a mechanism for securing or compromising information through the management of people and technology[49] and thus plays a vital role in organizational security[50]. In IBM's 2018 Cost of Data Breach study[51] clearly shows the need for effective organizational communication processes, as it is reported that it takes in average 197 days for organizations to detect a breach and a further 69 days to resolve the situation and restore service.

Many researchers conclude that managers should effectively communicate security-related concepts to their employees[52], yet little research empirically examines how such communication can affect later security behavior[53]. Empirical research on the role of communication in security culture is rare, but important: it shows that both the prevention of security breaches and the response to them are largely determined by effective communicative processes. Communicative structures (channels, possibilities to communicate) need to exist that give meaning and legitimation to desired practices[54].

There is a need for frequent communication within and between departments, possibly by a shared platform for interactions between employees. Where frequent communication is encouraged, employees who naturally would not communicate with others are presented with the opportunity to do so. More specifically, communication between departments needs to be collaborative, and it needs to be knowledge-rich communication. Collaborative communication is important both for security prevention and response strategies to achieve desired outcomes[55]. Information security is an inter-departmental effort rather than an IT-department-only effort, and inter-departmental collaboration requires a good communication culture[56].

Because annual security awareness training effectiveness decays over time, some employers and software vendors have begun to implement real-world short communications with some success[57]. Many sites now provide instant feedback on the strength of newly formed passwords, which has been shown to have a positive impact on user security behavioral outcomes[58]. Commercial web browsers utilise security warnings displayed to users who may surf to the wrong site[59]. And, the SANS Institute distributes Post-it notes that include the reminder "do not write your password here"[60].

Employee engagement is the result of an employee's cognitive and emotional motivation, self-efficacy to perform the job, a clear understanding of his or her role in the organization, and a belief that he or she has the resources to perform their job. All of these factors can be positively influenced through good communication.

While communication is a basic requirement of management, it is also instrumental in raising the morale of employees, affecting motivation, and encouraging employee engagement. It is through communication, verbal or non-verbal, that people submit different feedback and requirements to the management. Motivation plays a vital role in the discovery of the needs and aspirations of staff by managers. Proper

communication is an efficacious and proficient means to foster good human relationship with individuals (and the general public) and for keeping an organization proactive, in order to comfortably handle daunting challenges.

Other benefits of effective communication skills in building security culture are that communication acts as a source of information and helps in the decision-making process and helps in identifying the alternative course of action. As stated earlier, communication helps in building people's attitude. A well-informed person will always have better attitude than a less informed person. Different forms of communication like handbooks, newsletters and meetings will help the employees to form different attitudes. Communication also helps in the controlling process of management. It allows the managers to know about employees' grievances and helps the employees to know about the policies of the organization.

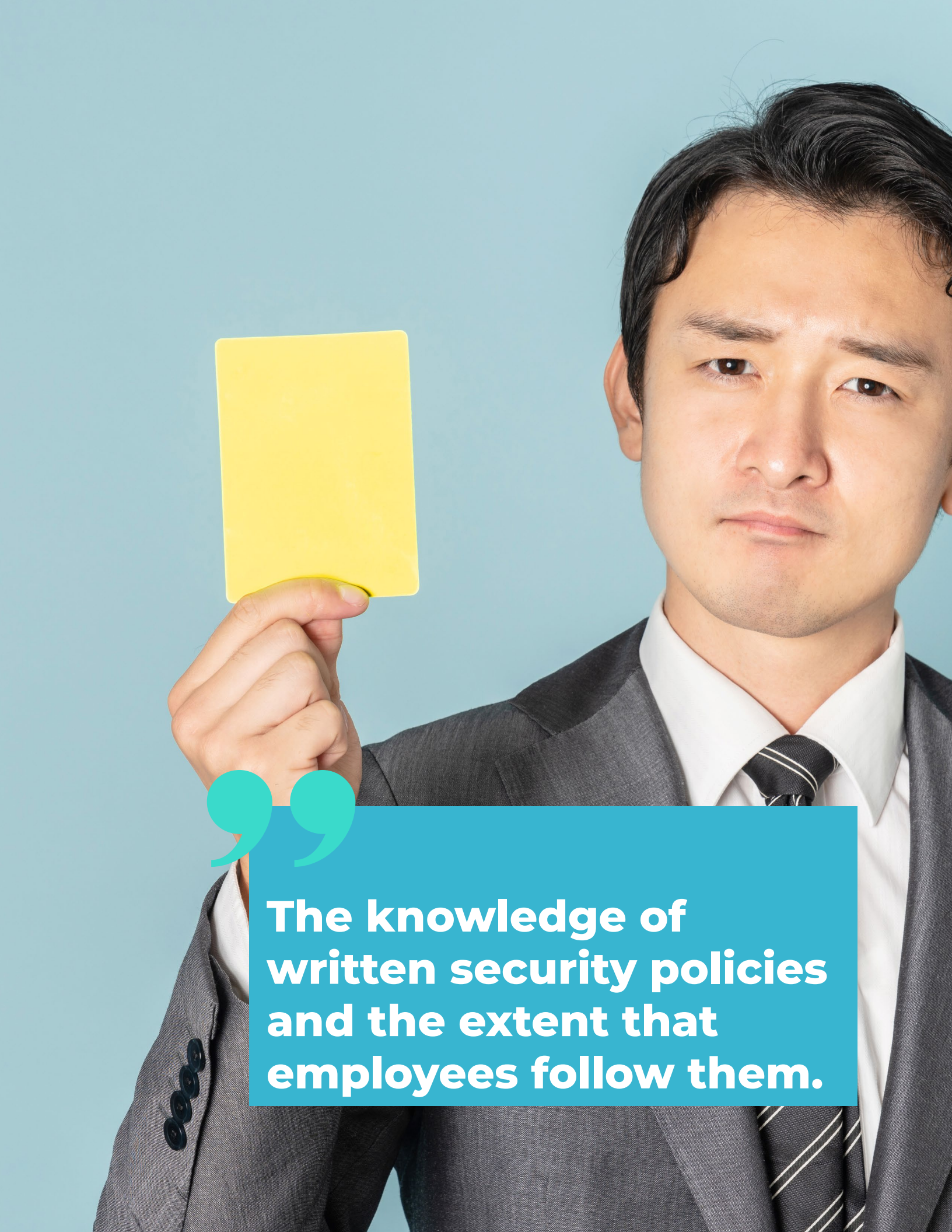
Effective communication is a necessary requisite for successful collaboration between departments and business units. A collaborative effort is needed to build an effective security culture and is a fundamental part of the Security Culture Framework (SCF). In particular, its Organization module (step two of the framework) requires that a security culture program "involve the right people and define target audiences"[61].

The SCF explains that the "right people" can be found from throughout the organization, in almost any department, at every level. Every successful security culture program needs to achieve executive buy-in and management commitment from the top down. In order to attain this, the core team (the main people who are going to design and implement your security culture program) will benefit greatly from multi-functional expertise. In addition to security expertise, for example, competences from marketing, communications and HR will be invaluable, as these roles require highly-developed communication channels with other stakeholders, including employees from across the organization. The "right people" can also be found in the form of potential security champions or ambassadors. Again, these people are not necessarily found inside the security or IT teams and can be found can be found from just about anywhere. Mapping the security culture of the organization against the organizational structure is one way to uncover potential security culture ambassadors.

Tips for positively influencing communication

Communication can be improved by various techniques, from improving the existing channels to improving sense-of-belonging through team building activities and other techniques such as:

- Resonate with your audience. Whether you are addressing senior management or front-line staff, it is important the information is provided in a way that is digestible and relevant to them. Listen to their concerns. Find out what is important to them and why. When explaining why certain security measures are important, be sure to communicate why they are important for them, for example, explain how the measure will affect their work, how will they benefit, and what impact it will have on them). Speak using language that resonates with your target audience.
- Keep members informed. Attitudes towards security measures are more likely to be built in a positive manner if members understand the necessity of the various steps that are made to secure the organization and its assets. Share what steps are being taken, why they're important, and what impact they will have (on the business as a whole, and on them individually).
- Encourage positive expression. The more often an attitude is expressed the stronger it becomes[62], whereas an attitude that is not expressed frequently is likely to be weakly held. Build a network of security ambassadors across different business areas. Encourage and support security champions.



The knowledge of written security policies and the extent that employees follow them.

Compliance

The knowledge of written security policies and the extent that employees follow them.

There is an abundance of scientific and professional research of information security compliance. This is not surprising as it is assumed that non-compliance to information security standards and policies is one of the main human-related reasons for security breaches in organizations[63]. Information security compliance ensures that information security mechanisms implemented in an organization work together effectively to protect the critical information[64]. It is considered to be an institutional yardstick to show that adequate steps have been taken to protect organizational information[65].

Enforcing information security compliance is a complex security culture issue[66]. Compliance includes many organizational processes. First of all, compliance assumes existence of information security policies (ISPs). Usually presented as a document, ISPs are a set of rules, regulations, laws and practices that state how assets in the system including sensitive information are managed, protected, shared and distributed accurately without any type of loss[67]. These policies typically describe the acceptable use of computer resources, the responsibilities regarding information security, and also the type of training that employees should have and the consequences of security policy violation.

Usually the main purpose of ISPs are to illustrate the employees' security responsibilities and roles and to describe procedures that should be followed to avoid the security risks[68]. They define a set of security rules and responsibilities of the employees to safeguard the information and technology resources of their organizations[69]. These policies must address the management, protection, and resources associated with the information and the Information Systems.

Compliance is not just about the existence of an adequate document, complied to by the employees, but also involves processes of communication, cooperation and coordination, so that the policies are adequately implemented and adhered to at all organizational levels. Adoption of information security compliance in organizations involves[70]:

(a) Implementation of effective and balanced information security measures and mechanisms.

(b) Compliance with legal and security requirements and expectations of organizations.

(c) Maintaining both employees' and stakeholders' confidence and trust in the security.

Having a well-documented set of policies and procedures is not, by itself, good enough to deter information security breaches[71]. It is imperative to define and understand factors that motivate and enhance employees' compliance with ISPs. Nowadays a number of different approaches exist that aim to identify the main factors of information security compliance in organizations.

The most commonly used approach is that of the Theory of Planned Behavior[72]. There are also other theories that focus on negative motivators, such as sanctions and fear[73]. Lately, research shows that the most effective seems to be intrinsic motivation rather than extrinsic

motivators[74]. This stream of research suggests that we should find a fit between the values of employees and the objectives of the ISPs, because intrinsic motivation to follow ISPs is much more effective than external ones, like sanctions. In any case, no conclusive results exist to suggest the best approach.

It is however clear that compliance with ISPs is deeply rooted in the security culture and wider organizational culture, which is why compliance is a complex socio-cultural phenomenon. Measuring compliance as a dimension of security culture is of utmost importance for organizational security.

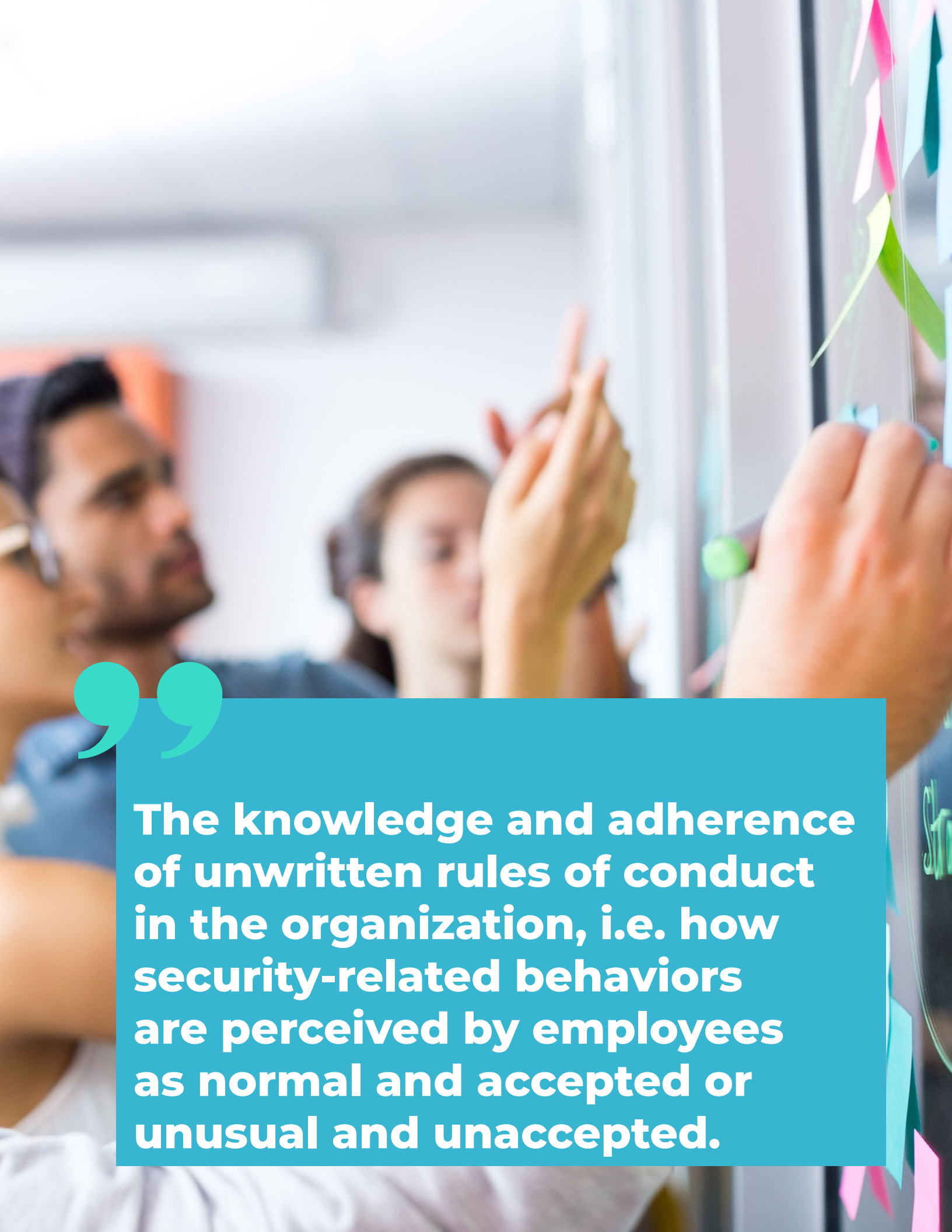
In addition to having a well-documented set of policies and procedures, ISPs must be clearly understood, readily available and easily accessible to all employees. Incorporating policy into learned processes and procedures is essential. Compliance can be improved when the employee understands how the policy affects them, their work activities and their role within the organization.

Moreover, measuring, monitoring and actively working to improve all dimensions of security culture, including Compliance, can have significant influence on improving employees' understanding and adherence to the information security policies set by an organization. In particular, we see that as levels of Cognition, Responsibilities, Communication, and Attitudes increase, Compliance is also positively impacted.

Tips for positively influencing compliance

Employees' understanding of and adherence to written policies can be improved by:

- ☐ Improving the quality of communication channels to discuss security-related issues and report incidents. (See Communication.)
- ☐ Increasing the understanding, knowledge and awareness of the policies themselves, including procedures to implement them into daily work tasks and activities. (See Cognition.)
- ☐ Strengthening the understanding of how important their own role is as a critical factor in sustaining or endangering the security of the organization. (See Responsibilities.)
- ☐ Supporting the attitudes towards the importance of security. (See Attitudes.)



The knowledge and adherence of unwritten rules of conduct in the organization, i.e. how security-related behaviors are perceived by employees as normal and accepted or unusual and unaccepted.

Norms

The knowledge and adherence of unwritten rules of conduct in the organization, i.e. how security-related behaviors are perceived by employees as normal and accepted or unusual and unaccepted.

Norms are widely understood to be one of the most important mechanisms that influence human behaviors[75], thus a key element of security culture. Just as norms in general help people negotiate their daily activities, we can say that organizational norms guide people in their daily conduct at workplace. Sociological, socio-psychological and behavioral information security research find that norms guide employees in their use of organizational infrastructure and IT[76], and emphasises norms as one of key influences of end-user security behaviors and compliance[77].

Norms can be internalised by various sensemaking systems[78]. Theory of Planned Behavior is a socio-psychological theory that has been quickly adopted by the security field and shows that people generally orient their activities on the basis of reasoning, i.e. "if other people who are important to me think I should do X, then it is probably smart to do X"[79].

However, the concept of norms is multidimensional and is not just about what other important people think. It is helpful to differentiate between two general types of norms, social norms and personal norms:

- Social norms can be defined as a set of (unwritten) rules that are based on common beliefs about how people act in a particular situation[80]. These are grounded in social interactions, and guide or restrain behavior through social sanctions, not the force of law. Social norms are enforced by informal rewards (like praise, reputation) and sanctions (ignorance, mocking).
- Personal norms on the other hand are internalised social norms. They are grounded in one's beliefs and values and their rewards and sanctions are self-imposed.

An individual who follows social norms, might do that in order to avoid sanction and not because he or she honestly believes that this is the right way of doing things. Conversely, an individual who follows personal norms does so because he or she believes that it is the normal and best way, and it is in line with his/her own values. Acting according to a personal norm becomes an end in itself rather than merely a tool in achieving certain goals or avoiding social sanctions[81].

Norms are very powerful, but also difficult to influence as they are relatively stable set of unwritten rules regarding what is good, right and important[82]. The task of a building security culture is thus to stimulate development of norms that support organizational security and ensure these norms become internalised. This way, adhering to a norm is intrinsically motivated and satisfying, and an individual will behave in line with norms even when there is no immediate social pressure or sanctions. This is because employees' values and behaviors are aligned with expectations that come from information security policies.

Unlike social norms, personal norms are difficult to manipulate directly. Stimulating pressure of personal norms should come from an employee's inner self and that is usually not easily accessible. Studies show that personal norms are influenced by external sources such

as social norms as well as factors such as awareness of consequences and ascription of personal responsibility[83]. Therefore, instead of directly appealing to employees' moral obligation, an organization may, via social norms, persuade its employees to behave accordingly.

Organizational norms are relatively stable social structures, but they can be changed. One important contextual factor is the general organizational culture, which first needs to establish an adequate moral climate[84], because human behavior is strongly affected by culturally transferred norms and values[85]. When policies are clearly communicated and accepted by the group, they help consolidate such pronouncements into normatively acceptable behavior.

Behavioral security research offers methods to measure norms, but they are somewhat limited, as these methods do not reveal the values behind norms. For example, an organization might develop a norm that it is completely acceptable to share passwords among employees when needed. Such norms will increase problematic end-user behavior. On the other hand, if organization has norms that instruct employees to mock people who write passwords on Post-It notes, such norms will probably positively influence end-user security behaviors, but have lasting damage to communication channels, employee attitudes and possibly responsibilities and compliance too. It is important to measure not only the presence of norms, but what kind of norms are present and how powerful are they.

Measuring norms in organizations is a key element of security culture program. This is as important as measuring behaviors, cognitions and other dimensions of security culture, if not more so. When a measurement tool detects a decline in norms that support security of organization, such change usually precedes changes in behaviors. Such observation is alarming but also allows management to inflict necessary changes before the changes in behaviors occur.

Studies show that personal norms are influenced by external sources such as social norms as well as factors such as awareness of consequences and ascription of personal responsibility[86]. Therefore, instead of directly appealing to employees' moral obligation, an organization may, via social norms, persuade its employees to behave accordingly.

Tips for positively influencing norms

Positive norms that support organizational security are internalised when employees' values and behaviors are aligned with those expected. Behaviors that are supportive of organizational security need to be identified, taught and reinforced. (See Behaviors.) When correct and expected behaviors are accepted as normal, adherence to these norms can be encouraged through the following mechanisms:

- Expectations can be set through information security policies and role responsibilities. When desired actions are clearly communicated and accepted by the group, they help consolidate policies into normatively acceptable behavior. (See Responsibilities.)
- Internal communication channels should be open and accessible to address any uncertainty and share best practices. Sharing lessons learnt, celebrating achievements, exemplifying correct behaviors, and acknowledging concerns are all proven mechanisms. (See Attitudes.)
- Design campaigns that advertise the information security related social norms. Encourage employees to share their stories using blogs, newsletters, and e-mails, etc, so that others become aware of the consequences of non-compliance and see others rewarded for adherence to norms. (See Communication.)
- In addition, the role of organizational punishment can be considered as a form of social control. When used as a legitimate deterrent, punishment facilitates distinction between desirable and undesirable acts and helps to establish group norms by identifying acceptable and unacceptable behaviors[87].

How employees perceive their role as a critical factor in sustaining or endangering the security of the organization.

Responsibilities

How employees perceive their role as a critical factor in sustaining or endangering the security of the organization.

Responsibility domain is mainly related to employees' practices and performance such as monitoring and control, reward and deterrence and acceptance of responsibility[88]. Employees should be aware that knowing and practicing secure behaviors is their responsibility[89]. Moreover, the protection of information should be part of the daily activities of the employees[90]. Employees need to be fully aware and committed to their role in the protection of the information in order to understand their responsibilities.

Organizations cannot truly protect their assets without ensuring that employees understand their roles and responsibilities, and they are sufficiently trained to perform them[91]. Employees can have knowledge of security issues, positive attitudes and generally good awareness of security issues, but they also need to be fully aware of their responsibilities and roles in securing their organization so that they are proactively engaged into resisting and reporting security incidents.

Every employee has a social and organizational role to play and these roles differ between employees and groups. Each employee has a set of expectations that are not general but tailored to each role. In other words, it is ineffective to target employees with security-related details that are irrelevant to their role[92].

Security responsibilities pertain to the social and organizational roles that employees have in the context of their organizational endeavors. Security research too frequently focuses exclusively on responsibilities of IT department and decision makers, while neglecting the responsibilities of 'ordinary' employees. The latter are usually not involved in the security issues, as research shows that only a small group of employees are involved in planning, managing and implementing security[93]. Consequently, employees do not feel that they play any important role in security issues and don't have any responsibility for security problems.

Awareness of roles and responsibilities is thus an important part of security culture. Moreover, an employee's awareness of their own individual security responsibilities, and their understanding of the importance of their responsibilities for the information security of the organization, is a key component of information security awareness concept as defined by the Information Security Forum.

Responsibilities can be influenced by clearly defining roles of employees regarding security. If the members of an organization do not understand their place in the security of the organization, they are less likely to follow the necessary steps and procedures to make the organization safe.

Tips for positively influencing responsibilities

In any organization, security is everyone's responsibility. How people understand those responsibilities is a key component of security culture. To improve, we offer the following advice:

- All members must understand that they are all a part of the security system, even if they are not working on sensitive material. This knowledge and understanding will make each and every member less likely to put the organization in danger through risky actions. (See Compliance.)
- Time should be taken to explain to every member of the organization how they fit into the security system of the organization. Because, when everyone is aware of their place within the organization's security, each person can more easily see how they can improve the security situation by their actions. (See Cognition.)
- Managers should make sure all members of their teams understand how the security system is a vital part of the organization and how they are all connected and responsible for securing their assets by acting responsibly and following the right procedures. (See Norms.)
- Managers should talk with the members of their teams regarding their responsibilities and how they can improve the security culture of the team and organization. Furthermore, managers should encourage dialogue between themselves, team members and security officers, to further knowledge of the responsibility they all have for the security situation of the organization. (See Communication.)

Supported by ENISA

Our approach is supported by the European Agency for Network and Information Security (ENISA). ENISA strongly recommends measuring security culture in its 2017 report entitled *Cyber Security Culture in Organisations*. In which, ENISA specifically lists the same seven human-related elements of organizational security that our security culture model is based on.

ENISA explains that, because organizations are complex social structures, a security culture transformation requires changing values and beliefs, altering behavior, and ultimately shaping underlying assumptions regarding security. It warns that "ignoring human factors in the development and deployment of cybersecurity policies and processes predestines [culture building] activities to failure."[94]

ENISA emphasises that, "before any further steps are taken, the current state of security culture in the organisation should be assessed."[95] Further advising that, in addition to establishing the level of knowledge and awareness of employees [i.e. **Cognition**], organizations should examine employee **Behaviors**, monitor employee activities to measure **Compliance**, study employee perceptions and understanding regarding some key aspects of cyber security culture, including "individual involvement and responsibilities regarding cybersecurity [i.e. **Responsibilities**], the effectiveness and openness of communication on the matter within the organisation [i.e. **Communication**]... employee beliefs and assumptions [i.e. **Attitudes**]... as well as what they perceive are the **Norms** of organisational conduct and practices within their company."[96] [Emphasis added.]

Endnotes

1 IBM 2018 Cost of a Data Breach Study
2 IBM 2018 Cost of a Data Breach Study
3 Greenberg, A., (2019, Jan 30)
4 IBM 2018 Cost of a Data Breach Study
5 Koulopoulos, T., (2017, May 11)
6 ENISA, 2018
7 Roer, et al (2013)
8 Roer (2015)
9 Herath & Rao (2009a)
10 Attitude objects can be a person, place, thing, or idea. Attitude objects are those things that a person makes a judgment about or has a feeling toward. These judgments or feelings about the attitude objects can be either positive or negative.
11 Jhangiani, Tarry, & Stangor (2014)
12 Banaji & Heiphetz (2010)
13 Jhangiani et al (2014)
14 De Houwer, Thomas, & Baeyens (2001)
15 Ashenden (2014)
16 Ashenden (2014)
17 Jhangiani et al. (2014)
18 Jhangiani et al. (2014)
19 Ajzen & Fishbein (2005)
20 Safa et al, (2016)
21 Safa et al., (2016); Tsohou et al., (2008); Siponen et al. (2014)
22 Abawajy (2014)
23 Hadlington (2018)
24 Bryce and Fraser (2014); Dinev and Hu, (2007)
25 Crossler et al., (2013); Herath & Rao (2009)
26 Safa et al., (2015)
27 Herath & Rao (2009b)
28 Stanton et al., (2004)
29 Sandler, R., (2018, May 29)
30 Wang, et al. (2018)
31 Crossler et al, (2013)
32 Crossler et al, (2013)
33 Safa et al., (2015)
34 Crossler et al, (2013)
35 For example, theories explored by Herath & Rao and Peace et al.
36 Herath & Rao (2009b)
37 Farooq & Vitanen (2015); Kajtazi & Bulgurcu (2013); Velki et al., (2017)
38 Lee, et al. (2016); Wang, P. A. (2010)
39 Kaur & Mustafa (2013)
40 Roer & Petric (2017). P.62
41 Farooq & Vitanen (2015)
42 Johnston, Warkentin, McBride, & Carter, (2016); Johnston et al., (2015)
43 Wang, P. A. (2010)
44 Wang, P. A. (2010)
45 Royce, (1974)
46 Farooq & Vitanen (2015)
47 Farooq & Vitanen (2015)
48 Farooq & Vitanen (2015)
49 Backhouse & Dhillon (1996)
50 Arhin & Wiredu, 2018; Pattinson & Anderson (2007)
51 IBM 2018 Cost of Breach Study
52 Boss, et al., (2015); Siponen & Vance (2010); Willison, Warkentin, & Johnston (2018)
53 Barlow et al. (2018)
54 Arhin & Wiredu (2018)
55 Arhin & Wiredu (2018)
56 Hoof et al., (2004)
57 Barlow et al. (2018)
58 Ciampa, (2013); Ur et al., (2012)
59 Anderson, Vance, Kirwan, Eargle, & Jenkins, (2016); Vance, Anderson, Kirwan, & Eargle, (2014)
60 Barlow et al. (2018)
61 https://securityculturefframework.net/category/framework/organization/
62 See Attitudes.
63 Al-Kalbani et al., (2014); Ullah et al., (2013)
64 Tassabehji et al., (2007); Kim et al., (2016)
65 Boss & Kirsch, (2007); Safa et al., (2016); Siponen et al., 2010)
66 Al Kalbani et al., (2014); Safa et al., (2016); Siponen et al., (2015)
67 Sidhu, (2012)
68 Al-Najjar, (2010)
69 Dulany, (2002)
70 AlKabani et al., (2017)
71 Safa et al., (2016)
72 Bulgurcu, Cavusoglu, and Benbasat (2010)
73 Kankanhalli et al., (2003)
74 Son, (2011)
75 Hechter & Opp (2001)
76 Cuganesan et al (2018)
77 Herath and Rao (2009b); Bulgurcu, Cavusoglu, and Benbasat (2010); Siponen, Pahnila, and Mahmood (2010)
78 Ekwutosi & Moses (2013)
79 i.e. Herath and Rao (2009a); AlHogail (2015); McGill and Thompson (2017)
80 Yazdanmehr & Wang (2016)
81 Gavrilets & Richerson (2017)
82 Bicchieri (2016).
83 Yazdanmehr & Wang (2016)
84 Yazdanmehr & Wang (2016)
85 Gavrilets & Richerson (2017)
86 Yazdanmehr & Wang (2016)
87 O'Reillys & Puffer (1989)
88 Al-Hogail (2017)
89 Al-Hogail (2015)
90 Thomson (2006)
91 Furnell & Thomson (2009)
92 Furnell & Thomson (2009)
93 Lim et al., 2009
94 ENISA (2018) p.30
95 ENISA (2018) p.40
96 ENISA (2018) p.41-42

Bibliography

Abawajy, J., (2014). User preference of cyber security awareness delivery methods. Behaviour and information technology, Vol. 33, pp. 237-248

Abdelwahed, A. S., Mahmoud, A. Y., & Bdair, R. A. (2016). Information Security Policies and their Relationship with the Effectiveness of the Management Information Systems of Major Palestinian Universities in the Gaza Strip. International Journal of Information Science and Management (IJISM), 15(1).

Ajzen, I. (1991). The theory of planned behavior. Organizational Behavior and Human Decision Processes, 50(2), 179–211.

Ajzen, I., Fishbein, M., (2005). The influence of attitudes on behavior. The handbook of attitudes 173 (221), 31

Albrechtsen, E., & Hovden, J. (2010). Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29(4), 432-445.

AlHogail, A. (2015). Design and validation of information security culture framework. Computers in Human Behavior, 49, 567-575.

AlHogail, A. (2017). Managing Human Factor to Improve Information Security in Organization.

AlKalbani, A., Deng, H., & Kam, B., (2014). A Conceptual Framework for Information Security in Public Organizations for E-Government Development, in Felix B Tan, Deborah Bunker (ed.) Proceedings of the 25th Australasian Conference on Information Systems (ACIS 2014) 1-11.

AlKalbani, A., Deng, H., Kam, B., & Zhang, X. (2017). Information Security compliance in organizations: an institutional perspective. Data and Information Management, 1(2), 104-114.

Al-Najjar, F.J. (2010). Management Information Systems - Administrative Perspective. Dar El-Hamed for publishing and distribution. Amman. Jordan.

Al-Omari, A., El-Gayar, O., and Deokar, A. (2012). Information security policy compliance: The role of information security awareness. AMCIS.

Anderson, B. B., Vance, A., Kirwan, C. B., Eargle, D., and Jenkins, J. L. (2016). How users perceive and respond to security messages: A NeuroIS research agenda and empirical study. European Journal of Information Systems, 25(4), 364-390.

Arhin, K., and Wiredu, G. O. (2018). An Organizational Communication Approach to Information Security. The African Journal of Information Systems, 10(4), 1.

Ashenden, D. (2018). In their own words: employee attitudes towards information security. Information & Computer Security, 26(3), 327-337.

Augoustinos, M., Walker, I., & Donaghue, N. (2006). Social cognition: an integrated introduction.

Aurigemma, S., and Mattson, T. (2014). Do it OR ELSE! Exploring the effectiveness of deterrence on employee compliance with information security policies.

Backhouse, J., and Dhillon, G., (1996). Structures of responsibility and security of information systems, European Journal of Information Systems, 5:1, 2-9.

Banaji, M. R., and Heiphetz, L. (2010). Attitudes. In S. T. Fiske, D. T. Gilbert, & G. Lindzey (Eds.), Handbook of social psychology [5],1,353–393. Hoboken, NJ: John Wiley & Sons.

Barlow, J. B., Warkentin, M., Ormond, D., and Dennis, A. R. (2018). Don't Even Think About It! The Effects of Antineutralization, Informational, and Normative Communication on Information Security Compliance. Journal of the Association for Information Systems, 19(8).

Bicchieri, C. (2016). Norms in the wild: How to diagnose, measure, and change social norms. Oxford University Press.

Boss, S. R., Galletta, D. F., Lowry, P. B., Moody, G. D., and Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. MIS Quarterly, 39(4), 837-864.

Bryce, J., & Fraser, J. (2014). The role of disclosure of personal information in the evaluation of risk and trust in young peoples' online interactions. Computers in Human Behavior, 30, 299-306.

Kirsch, L.J., and Boss, S.R. (2007). The Last Line of Defense: Motivating Employees to Follow Corporate Security Guidelines. Proceedings of the International Conference on Information Systems (ICIS).

Boss, S. R., Kirsch, L. J., Angermeier, I., Shingler, R. A. and Boss, R. W. (2009) If someone is watching, I'll do what I'm asked: mandatoriness, control, and information security, European Journal of Information Systems, 18, 2, 151-164.

Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (2010). Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness. MIS Quarterly, 34(3), 523-548.

Ciampa, M. (2013). A comparison of password feedback mechanisms and their impact on password entropy. Information Management & Computer Security, 21(5), 344-359.

Crossler, R. E., Johnston, A. C., Lowry, P. B., Hu, Q., Warkentin, M., and Baskerville, R. (2013). Future directions for behavioral information security research. Computers & Security, 32, 90-101.

Cuganesan, S., Steele, C., and Hart, A. (2018). How senior management and workplace norms influence information security attitudes and self-efficacy. Behaviour & Information Technology, 37(1), 50-65.

da Veiga, A. and Martins, N. (2015). Improving the information security culture through monitoring and implementation actions illustrated through a case study. Computers & Security, 49, pp.162-176.

De Houwer, J., Thomas, S., & Baeyens, F. (2001). Association learning of likes and dislikes: A review of 25 years of research on human evaluative conditioning. Psychological Bulletin, 127(6), 853-869.

Dhillon, G., Syed, R. and Pedron, C. (2016). Interpreting information security culture: An organizational transformation case study. Computers & Security, 56, 63-69.

Dinev, T., & Hu, Q. (2007). The centrality of awareness in the formation of user behavioral intention toward protective information technologies. Journal of the Association for Information Systems, 8(7), 23.

Dulany, K.M. (2002). "Security, It's Not Just Technical". SANS Institute-InfoSec Reading Room. Swansea. UK

ENISA, (2018, Feb 06). Cyber Security Culture in Organisations. Retrieved at: https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Farooq, A., Isoaho, J., Virtanen, S., and Isoaho, J. (2015, August). Information security awareness in educational institution: An analysis of students' individual factors. In Trustcom/BigDataSE/ISPA, 2015 IEEE (Vol. 1, pp. 352-359). IEEE.

Furnell, S. and Thomson, K. (2009). From culture to disobedience: Recognising the varying user acceptance of IT security. Computer Fraud & Security, 2009(2), 5-10.

Gavrilets, S., & Richerson, P. J. (2017). Collective action and the evolution of social norm internalization. Proceedings of the National Academy of Sciences, 114(23), 6068-6073.

Greenberg, A., (2019, Jan 30). "Hackers are passing around a megaleak of 2.2 billion records" Wired.com (blog). Retrieved from: https://www.wired.com/story/collection-leak-usernames-passwords-billions/

Hadlington, L. J. (2018). Employees Attitudes towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom. International Journal of Cyber Criminology, 12(1).

Hechter, M., & Opp, K. D. (Eds.). (2001). Social norms. Russell Sage Foundation.

Herath, T., and Rao, H. R. (2009a). "Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness". Decision Support Systems, 47(2), 154-165.

Herath, T., and H. Rao. (2009b). "Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations." European Journal of Information Systems 18 (2): 106–125.

Ifinedo, P. (2013). Information Systems Security Policy Compliance: An Empirical Study of the Effects of Socialization, Influence, and Cognition, Information & Management, 51(1), 69-79.

Jhangiani, R., Tarry, H., Stangor, C., (2014). Principles of Social Psychology-1st International Edition. Retrieved from: https://opentextbc.ca/socialpsychology/chapter/exploring-attitudes/

Johnston, A. C., and Warkentin, M., (2010). Fear Appeals and Information Security Behaviors: An Empirical Study. MIS Quarterly, 34(3), 549.

Johnston, A.C., Warkentin, M., and Siponen, M. (2015). An enhanced fear appeal rhetorical framework: Leveraging threats to the human asset through sanctioning rhetoric. MIS quarterly, 39(1), 113-134.

Johnston, A. C., Warkentin, M., McBride, M., and Carter, L., (2016) Dispositional and situational factors: influences on information security policy violations, European Journal of Information Systems, 25:3, 231-251

Kajtazi, M., and Bulgurcu, B. (2013). Information Security Policy Compliance: An Empirical Study on Escalation of Commitment. AMCIS 2013.

Kankanhalli, A., Teo, H. H., Tan, B. C. Y., and Wei, K. K., (2003). An integrative study of information systems security effectiveness, International Journal of Information Management 23 (2003) 139–154

Kaur, J., and Mustafa, N. (2013, November). Examining the effects of knowledge, attitude and behaviour on information security awareness: A case on SME. In Research and Innovation in Information Systems (ICRIIS), 2013 International Conference on (pp. 286-290). IEEE.

Kim, D.J., Hwang, I.H. and Kim, J.S., (2016). A Study on Employee's Compliance Behavior towards Information Security Policy: A Modified Triandis Model. Journal of Digital Convergence, 14(4), 209-220.

Koulopoulos, T., (2017, May 11). The Biggest Risk to Your Business Can't Be Eliminated – Here's How You Can Survive, Inc. (blog). Retrieved from: https://www.inc.com/thomas-koulopoulos/the-biggest-risk-to-your-business-cant-be-eliminated-heres-how-you-can-survive-i.html

Leach, J. (2003). Improving user security behaviour. Computers & Security, 22(8), 685-692.

Lee, C., Lee, C.C. and Kim, S., (2016). Understanding Information Security Stress: Focusing on the Type of Information Security Compliance Activity, Computers & Security, 59, 60-70.

Lim, J., Chang, S., Maynard, S. and Ahmad, A. (2009). Exploring the Relationship between Organizational Culture and Information Security Culture. In: Australian Information Security Management Conference. Perth, Western Australia: Proceedings of the 7th Australian Information Security Management Conference, 12.

McGill, T. and Thompson, N. (2017). Old risks, new challenges: exploring differences in security between home computer and mobile device use. Behaviour & Information Technology, 36(11), pp.1111-1124.

Merhi, M. I., and Midha, V. (2012). The impact of training and social norms on information security compliance: A pilot study. Proceedings of the International Conference on Information Systems (ICIS 2012).

Metalidou, E., Marinagi, C., Trivellas, P., Eberhagen, N., Skourlas, C. and Giannakopoulos, G. (2014). The Human Factor of Information Security: Unintentional Damage Perspective. Procedia - Social and Behavioral Sciences, 147, pp.424-428.

Myyry, L., Siponen, M., Pahnila, S., Vartiainen, T., and Vance, A. (2009). What levels of moral reasoning and values explain adherence to information security rules? An empirical study. European Journal of Information Systems, 18(2), 126-139.

O'Reillys, C., and Puffer, S. (1989). The impact of rewards and punishments in a social context: A laboratory and field experiment. Journal Of Occupational Psychology, 62(1), 41-53.

Pattinson, M. R. and Anderson, G. (2007). How Well Are Information Risks Being Communicated To Your Computer End-Users? Information Management and Computer Security, 15(5) 362 – 371

Parsons, K., Young, E., Butavicius, M., McCormac, A., Pattinson, M., and Jerram, C. (2015). The Influence of Organizational Information Security Culture on Information Security Decision Making. Journal Of Cognitive Engineering And Decision Making, 9(2), 117-129.

Pogarsky G. (2004) Projected offending and contemporaneous rule-violation: implications for heterotypic continuity. Criminology 2004;42(1):111-136.

Ponemon Institute. 2018 Cost of a Data Breach Study: IBM Security. Retrieved from: https://www.ibm.com/security/data-breach

Roer, K., and Petrič, G. (2017). Security Culture Report 2017 - In depth insights into the human factor.

Roer, K., et al. (2013). The Security Culture Framework. Retrieved from: https://securityculturefranework.net

Roer, K. (2015). Build a security culture. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing.

Royce, J. (1974). Cognition and Knowledge: Psychological Epistemology. In E. Carterette & M. Friedman, Historical and Philosophical Roots of Perception. Academic Press. Chp.9.

Safa, N. S., Sookhak, M., Von Solms, R., Furnell, S., Ghani, N. A., and Herawan, T. (2015). Information security conscious care behaviour formation in organizations. Computers & Security, 53, 65-78.

Safa, N. S., Von Solms, R., and Furnell, S. (2016). Information security policy compliance model in organizations. Computers & Security, 56, 70-82.

Sandler, R., (2018, May 29). "After Studying 6.1 Million Passwords, Researchers Identified the 6 Most Common Mistakes. Take a Look" Inc. (blog) Retrieved from: https://www.inc.com/business-insider/common-password-mistakes-how-to-choose-strong-password.html

Schwartz, M. J., (2017, Mar 3). "Verizon: Most Breaches Trace to Phishing, Social Engineering" Bank Info Security (blog): Information Security Group Corp. Retrieved from: https://www.bankinfosecurity.com/interviews/most-breaches-trace-to-phishing-social-engineering-attacks-i-3516

Sidhu, H. (2012). Fundamental Issues for Developing Information Security Policies. International Journal of Advanced Research in Computer Engineering & Technology (IJARCET). 1(10): 99-104.

Siponen, M., Mahmood, M. A., & Pahnila, S. (2014). Employees' adherence to information security policies: An exploratory field study. Information & Management, 51(2), 217-224.

Siponen, M., Pahnila, S., & Mahmood, M. A., (2010). Compliance with Information Security Policies: An Empirical Investigation. Computer 43 (2): 64–71.

Siponen, M. & Vance, A. (2010). Neutralization: New insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), 487-502.

Stanton, J. M., Stam, K. R., Mastrangelo, P., Jolton, J., Analysis of end user security behaviors. Computers & Security, 24.2 (2005): 124-133.

Son, J. Y. (2011). Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies. Information & Management, 48(7), 296-302.

Tassabehji, R., Elliman, T., and Mellor, J. (2007). Generating Citizen Trust in E-Government Security: Challenging Perceptions, International Journal of Cases on Electronic Commerce, 3(3), 1-17.

Tischer, M., Durumeric, Z., Foster, S., Duan, S., Mori, A., Bursztein, E., and Bailey, M. (2016, May). Users really do plug in USB drives they find. In IEEE Symposium on Security and Privacy (SP), 2016. IEEE. 306-319

Thomson, K., von Solms, R., & Louw, L. (2006). Cultivating an Organizational Information Security Culture. Computer Fraud & Security, 2006(10), 7-11.

Tsohou, A., Kokolakis, S., Karyda, M., and Kiountouzis, E., (2008) Process-variance models in information security awareness research. Information Management & Computer Security, 16(3), 271-287.

Ullah, K. W., Ahmed, A. S., & Ylitalo, J. (2013). Towards Building an Automated Security Compliance Tool for the Cloud. IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 8, 1587-1593.

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., et al. (2012). How does your password measure up? The effect of strength meters on password creation. In Proceedings of the 21st USENIX Security Symposium (USENIX Security 12). ACM. 65-80.

Vance, A., Anderson, B., Kirwan, B., Eargle, D. (2014). Using measures of risk perception to predict information security behavior: Insights from electroencephalography (EEG), Journal of the Association for Information Systems, 15(10), 679-722.

Wang, P. A. (2010, June). Information security knowledge and behavior: An adapted model of technology acceptance. In Education Technology and Computer (ICETC), 2010 2nd International Conference on (Vol. 2, pp. V2-364). IEEE.

Wang, et al. (2018) The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services. Retrieved from: https://people.cs.vt.edu/gangwang/pass.pdf

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. Information Systems Journal, 28(2), 266-293.

Yazdanmehr, A., & Wang, J. (2016). Employees' information security policy compliance: A norm activation perspective. Decision Support Systems, 92, 36-46.

CLTRe
a KnowBe4 company

> **You cannot improve what you do not measure.**

https://www.knowbe4.com/resources