







A Cyber-Security Culture Framework for Assessing Organization Readiness

Anna Georgiadou , Spiros Mouzakitis , Kanaris Bounas , and Dimitrios Askounis 

National Technical University of Athens, Athens, Greece

ABSTRACT

This paper presents a cyber-security culture framework for assessing and evaluating the current security readiness of an organization's workforce. Having conducted a thorough review of the most commonly used security frameworks, we identify core security human-related elements and classify them by constructing a domain agnostic security model. We then proceed by presenting in detail each component of our model and attempt to quantify them in order to achieve a feasible assessment methodology. The paper thereafter presents the application of this methodology for the design and development of a security culture evaluation tool, that offers recommendations and alternative approaches to workforce training programs and techniques. The model has been designed to easily adapt on various application domains while focusing on their unique characteristics. The paper concludes on applications of our instrument on security-critical domains, and its contribution to current research by providing deeper insights regarding the human factor in cybersecurity.

KEYWORDS

Cybersecurity culture; assessment; awareness; security behavior

Introduction

Information Security is a multidisciplinary area of study and professional activity focusing on safeguarding and protecting Information Technology against a variety of dangers and threats.^{1,2} Initially, information security was characterized by a rather technical approach best left to the technical experts.³ Even at this early stage, people responsible for implementing information security, identified the need for top management becoming involved. This led to a second phase where information security was incorporated into organizational structures and Information Security Managers were appointed.⁴ Security policies and procedures were drafted creating the need to understand their effectiveness and assess their results. But most importantly, revealing that there were other elements of information security that had been disregarded up until then. Information security standardization, certification and assessment were introduced along with an effort to understand and address the human element as an important security factor.⁵

An organization's biggest threat to privacy and security, even if not acknowledged, are considered to be their own staff.⁶ Employee security awareness is a key link to an organization's security chain since even the most well-guarded corporation is defenseless with no security culture.^{7,8} This term, "security culture," soon dominated in the era and was attributed various definitions.⁹ The vast majority of them agree that it "exists when every participant in the information society, appropriately to their role, is aware of the relevant security risks and preventative measures, assumes responsibility and takes steps to improve the security of their information systems and networks."^{10(p.8)}

Security culture is cultivated via a long and time-consuming procedure affected by various factors with different weights.^{11-19,20} And, although, certain information security assessment techniques are established, the same does not apply for the evaluation methods used by its corresponding culture.^{21,22}

Driven by the importance of this undoubtedly significant cyber-security factor, the underlying research focuses its efforts on designing a generalized security culture framework able to adapt to different domains and adjust its assessment methodology accordingly. A model depicting the core security culture levels, dimensions, and domains has been designed based on previously conducted scientific research while filling the gaps and inabilities among the different approaches. To intercept the cultural status of an organization and, at the same time, pinpoint the neglected security regions the most widely used assessment methods have been used: testing, examination, and interviewing.^{21,23} Our framework thereafter outlines linking the results of the assessment with valuable recommendations and practical ways of enforcing organizational and individual awareness, commitment, and engagement toward cyber-security. Thus, through continuous assessment iterations, the ultimate goal is to diminish the human-related cyber-threats against an organization.

This paper presents a methodology for evaluating the cyber-security culture of an organization with an emphasis on the aspects of the human factor. Section 2 presents background information regarding current research studies as well as leading standards and frameworks on cybersecurity behavioral analysis as well as their relation to crucial security hazards. Building upon the wide and diverse range of these studies a holistic, security culture model is presented in

Section 3, in an effort to develop an innovative instrument for the assessment of the cybersecurity readiness of a company with an emphasis on the human factor. The model depicts the core security factors per different levels, dimensions, and domains, in detail. Furthermore, we describe how our framework assesses the impact of each security factor on the overall security culture readiness level. In Section 4, we present how the specific instrument can be applied in practice on different business domains as well as our first applications aiming at the critical EPES¹ sector. In Section 5, we outline a number of considerations and limitations regarding the proposed model. Finally, Section 6 concludes with the importance and impact of our proposed framework for enterprises as well as areas of further research and potential future applications.

Background

Scientific research perspective

The complexity of the human nature with regard to information security has long been a subject of research for different scientific disciplines. Their goal was to approach, understand, and finally analyze how the employee's feelings, beliefs, behavior, attitude, and actions can directly or indirectly, intentionally or unintentionally, affect and possibly threaten the information security of an organization. Understanding the basis of the problem could lead to effective solutions: applicable and fruitful security policies and procedures as well as training programs that could contribute to cultivating a prosperous security culture.

Employees' adherence to information security policies served as the starting point for many scientific surveys exploiting various theories, such as the Theory of Planned Benefits (TPB), the Rational Choice Theory (RCT), the Protection Motivation Theory (PMT), the General Deterrence Theory (GDT), the Social Cognitive Theory (SCT) and the Theory of Reasoned Action (TRA).^{24,25} Intention to comply with information security policies proved to be fundamentally affected by employees' attitude, normative beliefs, and habits whereas sanctions and intention had a significant impact on actual compliance to them.²⁶ Threat appraisal and facilitating conditions were found to have a positive influence while coping appraisal and sanctions would have negative or even no influence at all.²⁷

Evidence that individuals who have both the security knowledge and skills may fail to efficiently apply them to their daily working routine triggered another research notion aiming to explore relationships among self-efficacy in information security, security practice behavior, and motivation.²⁸ Self-efficacy, in the context of information security, refers to an employee's self-confidence in their skills or ability to comply with the controls taken by the organization.²⁹ Research showed that people with high-efficacy demonstrate a higher degree of conviction about their ability to mobilize motivation and cognitive resources needed to successfully execute the guidance of the organization's information security policies.³⁰ At the same time, habits and subjective norms

were found to directly influence actual behavior and reduce the impact of behavioral intentions to comply with organizational security policies.³¹

Although findings revealed the need for security technology to be user-centered in order to be effective, they also underlined that social and working environment around an individual has an apparent impact on one's security behavior and compliance.³² Scholars focused on bridging the gap between individual intent and actual behavior given a specific working reality and information security approach.^{26,27,29,31} Robert E. Crossler et al., Zahoor Ahmed Soomro et al., Qing Hu et al. are some of the researchers who identified the need to co-examine the organizational and individual level factors effecting and shaping the organizational culture and, therefore, directly influencing information security outcomes, paving the way for further scientific research.^{33–35} The need to study, investigate and, finally, quantify organizational and individual security dimensions along their many interactions and interdependencies in a formalized way arose.

Information security standards and professional frameworks

In parallel, the professional society focused on designing security assessment frameworks as a means of creating the business, environmental, and social conditions that would form the foundations for a proper and promising security culture.

Efforts on this field started much earlier when in 1995 BSI Group published BS 7799 as a standard. Its first part contained best practices for information security management while its second part, titled "Information Security Management Systems – Specification with guidance for use", focused on how to implement an information security management system (ISMS). Both parts were later on adopted by ISO and incorporated in the ISO 27000 series of standards as ISO/IEC 27002:2007 and as ISO/IEC 27001:2005 respectively.^{36,37} Together, they form what is probably one of the most widely adopted security recommendations.

A year later, Information Systems Audit and Control Association (ISACA) released COBIT. COBIT, standing for Control Objectives for Information and Related Technology, was a framework designed to bridge the crucial gap between technical issues, business risks, and control requirements.³⁸ It soon became a thoroughly recognized guideline applicable to any organization in any industry. Overall, it is being used to ensure quality, control, and reliability of information systems in an organization.

In 2005, a new comprehensive information security approach named PROTECT was introduced. Its name was an acronym for the seven control components (Policies, Risks, Objectives, Technology, Execute, Compliance, and Team) suggested as the core elements of an effective security program and was aiming at addressing all aspects of information security.³⁹

¹Electrical Power and Energy System.

In 2007, A. Da Veiga and J. H. P. Eloff presented the Information Security Governance framework to be used as a starting point by an organization to minimize risk and cultivate an acceptable level of information security culture.⁵ It addressed technical, procedural, and human components while allowing further adjusting for the varying national and international legislation and regulations that each organization is subject to.

A few years later, National Institute of Standards and Technology (NIST) issued Special Publication (SP) 800–53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations.⁴⁰ Its main purpose was to provide guidelines for selecting and specifying security controls for information systems supporting executive agencies of the federal government.

In 2017, ENISA, taking into consideration the academic and research community's notion and findings which was conducted in parallel, differentiates for the first time the professional society approach by publishing the Cybersecurity Culture (CSC) Framework. According to CSC, the concept of cybersecurity culture refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms, and values of people regarding cybersecurity and how they manifest themselves in people's behavior with information technologies.⁴¹ Soon, a security toolkit was developed based on its principles and guidelines, the Security CLTRe Toolkit,⁴² which enables an organization to evaluate and graphically represent their security cultural status by means of seven specific dimensions. This was the first formalization attempt of the scientific approach to the human security factor.

Up until then, security professionals focused on designing security standards and frameworks aiming at security infrastructure, policies, and procedures safeguarding workplaces and employees but without practically encouraging individual engagement, participation, and awareness. Most importantly, suggested frameworks neglected employee intent and actual behavior while trying to conform and comply to the information security controls and suggestions formulated within a business environment.

On the other hand, as presented in the previous section, academic research approached cyber-security via anthropological and social studies meant to understand how environmental factors, individual features and traits affect, induce and finally dictate the overall information security of an organization. The potential of combining these two seemingly incompatible but actually supplementary security approaches is yet to be explored. This paper focuses on combining scientific results and business findings while bridging their diversities. Its final goal being none other than designing, implementing, and finally proving a robust **security culture framework** able to evaluate and meaningfully contribute to the improvement of the security reality of an organization.

Security culture framework

Model

Having conducted a multidisciplinary research review and thoroughly studied several academic principles and security expert

approaches towards information security, including technical analyses, algorithmic frameworks, mathematical models, statistical computations, behavioral, organizational, and criminological theories, we have created a foundation combining the elements that constitute the critical cyber-security culture factors. Combining human-centric elements and attributes with organizational, both external and internal, parameters, we have concluded in designing a globalized model.

This draft model was then presented and discussed in a series of workshops with security professionals and academic experts with specialization on information security in the context of the EnergyShield initiative during the first year of the project implementation.⁴³ Representatives of software companies implementing security solutions and industrial products, cybersecurity consultant organizations and university departments related to information security participated and dynamically contributed in finetuning and finalizing our model reaching to its first robust version presented in [Figure 1](#).

More specifically, this model clearly defines two levels: **organizational level** is meant to encompass all factors related to an organization's security technological infrastructure, operations, policies, and procedures while **individual level** is targeted on employee's attributes and characteristics with immediate impact on their security attitude and behavior. This way, both perspectives presented so far are enclosed and suggested model manages to combine both "external" human factors as well as "internal" driven individual notions.

Each level is then broken down into different **dimensions**. Organizational level is divided into dimensions that include the designing, development, documentation, and implementation of security policies and procedures that aim at different business domains. More specifically:

Assets: refers to the organization's assets (including people, buildings, machines, systems, and information assets) and includes policies that enforce several levels of confidentiality, availability, and integrity controls.

Continuity: is meant to ensure operations, services, and production continuity for an organization at predefined levels while safeguarding the reputation and interests of key stakeholders in cases of disruptive incidents.

Access and Trust: focuses on appropriate access to resources across the organization while clarifying different roles and permissions. In addition, it delimits any interactions the organization has with third-party factors, such as suppliers, customers, authorities, and so on.

Operations: refers to the administration of business practices to create the highest level of efficiency possible within an organization while taking into account the security aspects that safeguard its final results.

Defense: focuses on the foresight to have planned, acquired, and properly configured all technical assets necessary for the improvement and efficient operation of its information security.

Security Governance: refers to the measures taken to effectively plan, manage, and improve its information security.

On the other hand, individual level is consisted of the following dimensions:

Attitude: refers to the feelings and beliefs employees have toward security protocols and issues.

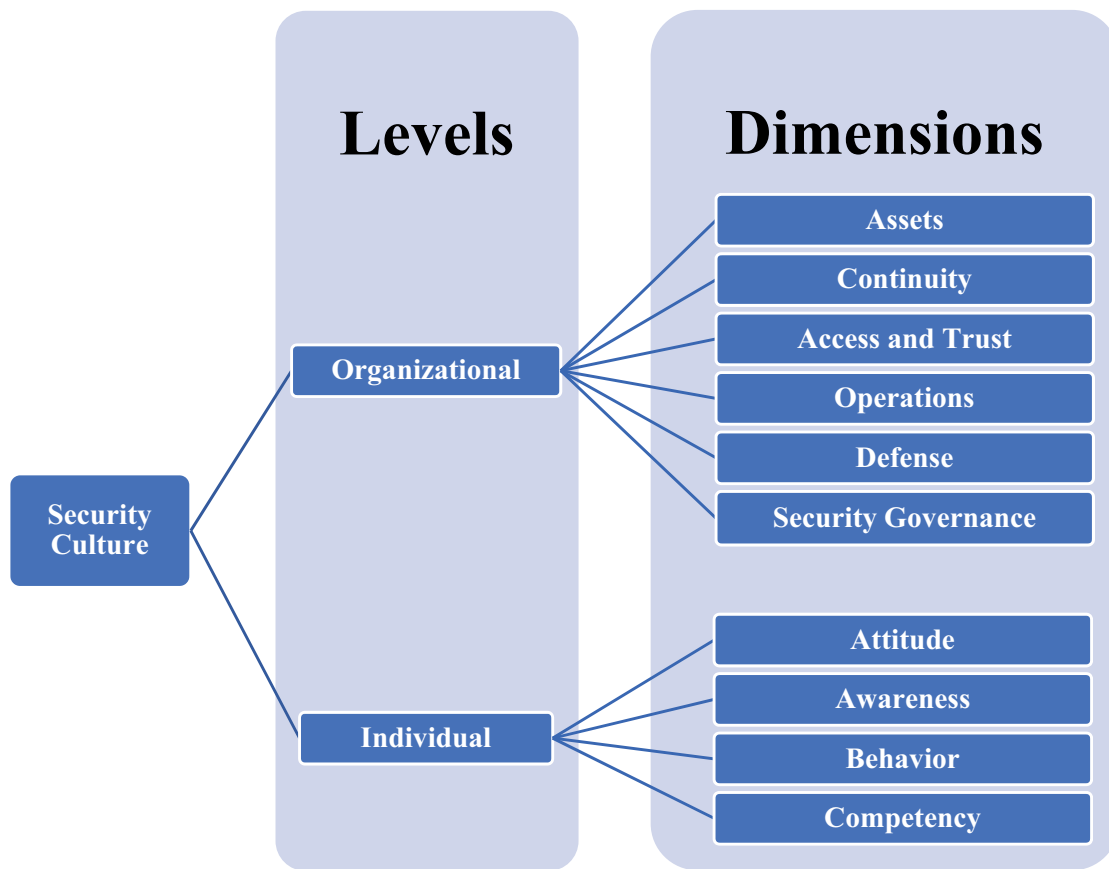


Figure 1. Cyber-security culture model.

Awareness: examines employees' understanding, knowledge, and awareness of security issues and activities.

Behavior: studying the security-conscious behavior exhibited on a day-to-day basis in an individual's workplace.

Competency: evaluating the employees' abilities, skills, knowledge, and expertise that enable them to conform with the security policies and procedures of the organization.

Each dimension is in turn analyzed into **domains** with distinctive application areas and quantifiable indicators. Table 1 holds a brief presentation while correlating them with the established research results were their basis lies.

Each domain is then broken down to a number of controls that vary from simple yes/no, likert scale, or multiple questions to quantitative and qualitative ones. Each control bears different weights to the domain assessment result so as to attribute the different importance and, thus, impact specific factor has in the overall security culture formation.

Controls are being evaluated using different techniques depending on their nature and significance⁸⁵:

- Questionnaires, widely used for the organizational level domain controls, remain brief, easy-to-understand, and targeted to facilitate interviewees.
- Simulations cover a wide range of artifacts such as phishing e-mails, social media fraud techniques, workstation virus contamination and so on.
- Tests varying from real-time user-targeted ones, such as password robustness, e-mail exposure, ransomware resilience,

and extended organizational-aimed ones, such as domain spoofing, mail server resistance and various others.

- Serious games are being used not only as a more reliable evaluation method but also due to their instructive nature and impressive effectiveness results.

- Simple observation, reporting from different sources and cross-analysis of the collected information is also invoked.

The suggested model applies to any size and kind of organization regardless of its business domain, specialization, technological status, and security readiness. It can also be used by any operational structure demonstrating a definite distinction between a decision-making board and a production unit. It can be adjusted to any business field by calibrating metrics defined for each of its domains. Additionally, it can be expanded and updated with little effort to constantly keep pace with the continuously transforming business environment.

Scientific findings on different professional domains suggest that each security factor contributes with a different weight in the overall security culture of an organization. Therefore, the scoring methodology needs to be dynamic by adjusting to the specific needs of the business field in the framework is being applied. The use of different techniques to attribute the individual security factors is suggested starting from a simple weighted average/sum method and leveraging to more sophisticated multi-criteria analysis methods, including pairwise comparison methods such as the Analytic Hierarchy Process (AHP) or the PROMETHEE family,^{86,87} outranking methods like the ELECTRE family,⁸⁸ or distance-based methods like TOPSIS

Table 1. Cyber-security model correlation to established research results.

Level	Dimension	Domain	Definition	Sources	
Organizational	Assets	Application Software Security	Management of the security life cycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.	36,37,44,45	
		Data Security and Privacy	The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.	37,44-47	
		Hardware Assets Management	Active documentation, inventory and management of all hardware devices or physical assets so that effective protection is assured.	36,37,44,48	
		Hardware Configuration Management	Establishment, implementation, and active management of security configuration for all hardware devices or physical assets using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.	44,45,48	
		Information Resources Management	Classification of all information assets depending on their criticality, confidentiality, and business value.	48,49	
		Network Configuration Management	Establishment, implementation, and active management of network infrastructure devices security configuration using a rigorous management and change control process to prevent attackers from exploiting vulnerable services and settings.	36,37,44,45	
		Network Infrastructure Management	Management of the ongoing operational use of ports, protocols, and services on networked devices to minimize vulnerability windows available to attackers.	44	
		Software Assets Management	Active documentation, inventory, and management of all corporate software assets so that effective protection is ensured.	36,37,44,48	
		Personnel Security	Management of the proper authentication and authorization level controlling personnel and/or visitors' access in the physical facilities of the organization.	36,37,46,47,50-52	
	Continuity	Physical Safety and Security	Establishment, implementation, and active management of facilities' physical security.	36,37,45,46,49	
		Backup Mechanisms	The backup procedures used to avoid loss of critical information and provide a level of acceptable business continuity in case of incidents.	36,37	
		Business Continuity & Disaster Recovery	The processes and tools used to properly back up critical information with a proven methodology for its timely recovery.	36,37,44-46	
		Capacity Management	The procedures with which the organization can ensure that information technology resources are right sized to meet current and future business requirements in a cost-effective manner.	36,37	
		Change Management	The procedures used for the management of any changes, internal and external, in the organization.	36,37,53-57	
		Continuous Vulnerability Management	Continuous acquisition, assessment, and elaboration on new information to identify vulnerabilities, remediate, and minimize the opportunity window for attackers.	44	
		Access and Trust	Access Management	The processes and tools used to track, control, prevent, and correct secure access to critical assets according to the formal determination of which persons, computers, and applications have a need and right to access these critical assets based on an approved classification.	36,37,44,45,48
			Account Management	Active management of system and application accounts' life cycle to minimize opportunities for attackers to leverage them.	36,37,44,46
			Communication	Various controls aiming to protect data, information, and systems during communication procedures.	36,37
	External Environment Connections		Establishment and active management of the external environment connections of the organization.	49	
	Password Robustness and Exposure		The measures taken by the organization to ensure password robustness along with the policies safeguarding confidentiality.	36,37,47	
	Privileged Account Management		The processes and tools used to track, control, prevent and correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.	36,37,44	
	Role Segregation		The proper appointment of roles and responsibilities ensuring their segregation in various processes and procedures to avoid possible conflict of interests.	36,37	
	Third-Party Relationships		Determination of the necessary requirements a third party should have to be considered trusty, along with the implementation of the necessary procedures with which those requirements are fulfilled.	36,37,49,58-60	
	Wireless Access Management		The processes and tools used to track, control, prevent and correct the secure use of wireless local area networks (WLANs), access points, and wireless client systems.	36,37,44,45	
	Operations	Compliance Review	Controls determining the security level appointed by security audit results.	36,46	
		Documentation Fulfillness	All the necessary documentation an organization is advised to have to maintain an appropriate level of information security.	36,37	
		Efficient Distinction of Development, Testing and Operational Environments	Proper segregation of the development, testing and operational environments.	36,37,61	
Operating Procedures		Definition of operating procedures with focus on minimizing the possibility of errors and malpractices.	36,37		
Organizational Culture and Top Management Support		Identification, establishment, and active management of the organizational culture and top management support influencing and formatting the overall security culture of the organization.	37,45,49,60		
Risk Assessment	Risk assessments to identify organization vulnerabilities repeated at regular intervals or when significant changes occur.	37,59,61-63			

(Continued)

Table 1. (Continued).

Level	Dimension	Domain	Definition	Sources
Individual	Defense	Boundary Defense	Detection, prevention, and correction of the information flow transferring across networks of different trust levels with a focus on security-damaging data.	44
		Cryptography	Cryptographic controls used by the organization.	36,37
		E-Mail and Web Browser Resilience	Minimization of the attack surface and the opportunities for attackers to manipulate human behavior through their interaction with web browsers and e-mail systems.	44,48,58
		Information Security Policy and Compliance	Establishment, implementation, and active management of information security policies and the compliance to them.	37,49,57,62,64–66
		Malware Defense	Controls over the installation, spread, and execution of malicious code at multiple organization points, while optimizing the use of automation to enable rapid updating of defense, data gathering, and corrective action.	36,37,44
	Security Governance	Security Awareness and Training Program	Specific knowledge, skills, and abilities' identification needed to support defense of the organization; development and execution of an integrated plan to assess, identify gaps, and remediate through policy, organizational planning, training, and awareness programs.	44,46–48,50,67–71
		Audit Logs Management	Collection, management, and analysis of event logs that could assist in detecting, understanding, or recovering from attacks.	36,37,44
		Incident Response and Management	Protection of the organization's information, as well as its reputation, by developing and implementing an incident response infrastructure.	36,37,44,48,49
		Penetration Tests and Red Team Exercises	Testing the overall strength of an organization's defense by simulating the objectives and actions of an attacker.	44,45,58
		Reporting Mechanisms	The channels used by the organization for employees or other relevant parties to report vulnerabilities or incidents detected.	36,37,48,67
	Attitude	Security Management Maturity	Controls evaluating the security management maturity of an organization.	37,49,62,72
		Employee Climate	The assessment of the satisfaction each employee has toward information security, directly affecting his/her security behavior.	33,51,52,73–76
		Employee Profiling	A generic employee profile that shall assist in identifying possible security behavioral patterns.	33,77–80
		Employee Satisfaction	The assessment of the satisfaction each employee has toward both the organization and other colleagues directly affecting his/her security behavior.	5,36,37,53,55,68,79
		Awareness	Policies and Procedures Awareness	Assessment of the cognition each employee has regarding the organization's security policies and procedures.
	Roles and Responsibilities Awareness		Assessment of the cognition each employee has regarding his role and responsibilities related to information security.	7,36,37
	Behavior	Policies and Procedures Compliance	Controlling and logging any security policies and procedures incompliance or violations by employees or other affected parties.	36,37,62,73,82
		Security Agent Persona	Identification of the kind of security-conscious behavior individuals tend to exhibit on a day-to-day basis in their workplace.	77,83
		Security Behavior	Security-conscious behavior exhibited on a day-to-day basis in the workplace.	7,74
	Competency	Employee Competency	The identification and definition of the competency needed for each role and responsibility along with the documented proof of competency each employee bears.	36,37
Security Skills Evaluation Training Completion and Scoring		Security skills, familiarity, and awareness evaluation. Record of any training programs attended by individuals along with scoring, completeness rate and assessment of their effectiveness.	65,79,84 36,37	

and VIKOR.⁸⁹ This intelligence should then serve as the basis for a designed and rightfully trimmed security analysis leading to targeted awareness and training programs along with other information security policies' adjustments and modifications.

Evaluation methodology

The proposed model represents the key security metrics to be measured along with their dependencies, influences, and varieties. The next step is to define an evaluation methodology that not only shall enable an organization to illustrate a uniform representation of its everyday reality but shall also assist in identifying its vulnerabilities and weaknesses. Knowledge based on figures and numbers is a powerful decision-making asset.

As depicted in Figure 2, the evaluation methodology consists of clearly defined and easily comprehensible steps. Starting from the decision of performing a security assessment process either due to an organization board's initiative or

(which is usually the case) driven by the need to defend against the numerous cyber threats of current reality (possibly after an unexpected real-life incident). The decision-making group, bearing in mind the real reasons behind this endeavor, need to set the initial goals and provide proper business requirements. Depending on their expectations, the entire methodology shall be, respectively, targeted in means of groups and security domains.

In the next step, evaluation iterations, so-called **assessment campaigns**, are being planned by managers and team leaders with proper variations among the different user groups, teams, or even organization sections and departments. Bearing in mind the targeting results of the previous step, they calibrate and carefully and collaboratively design the **evaluation procedure** which takes place in the next step. Using proven techniques, such as testing, examination, interviewing,^{21,23} simulation, gamification, and many others,⁸⁵ gather as much information as possible from its participants.

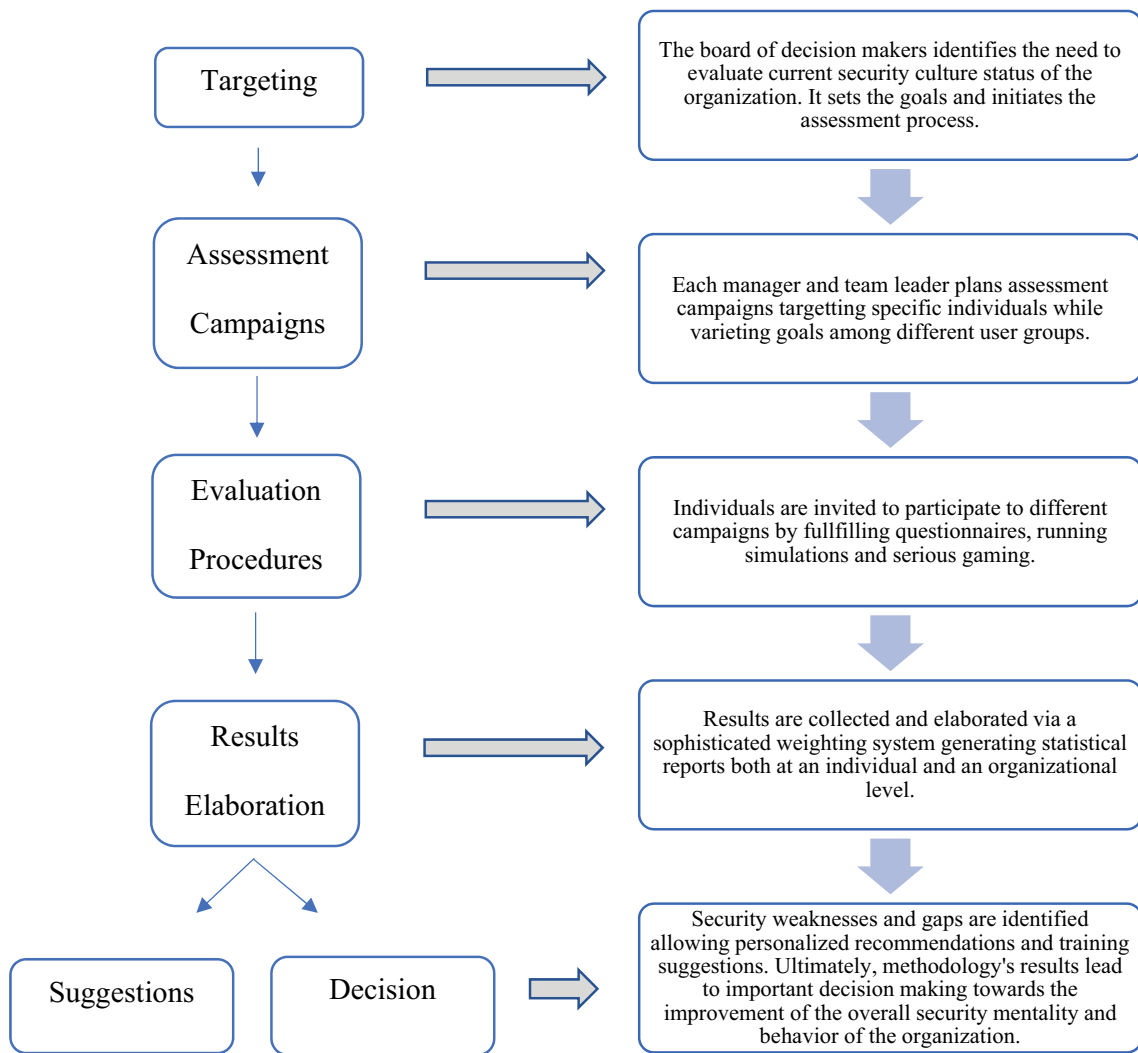


Figure 2. Security culture evaluation methodology.

Reaching to the most demanding step of the methodology, results are being gathered and analyzed via a series of sophisticated weighting algorithms and statistical computations generating a number of graphical representations and reports at an individual as well as organizational level. Using the score generated by the evaluation procedure for each targeted **individual** (analyzed into the different dimensions and domains), the methodology proceeds in appropriately aggregating them along with the **organizational** related ones producing corresponding scores for sections, departments, units, and ultimately for the organization as a whole.

Finally, acquired results pinpoint the existing security weaknesses and gaps allowing security training programs' personalization and adaptation to user-specific needs. Suggestions and recommendations are being provided both to individuals and directors while decision-making board is armed with the knowledge of their security culture status along with its pain points.

An indicative-simplified scenario to serve as an example of all of the above would be as follows. The security officers of company X have been alerted by the security operation center (SOC) solution at hand that an excessive number of

fraud e-mails are reaching their marketing department. After further investigating, have also verified a misuse of social channels from its employees. Consequently, they have reached the decision to run an assessment campaign targeting this specific department. Since their focus lies on the e-mail, web, and social media usage, they include to their campaign a number of relative questionnaires, phishing simulation tests, social engineering games, and e-mail, and password exposure checks. After the expiration date of the campaign, the security officers gather the results and via a graphical representation are able to understand both the security vulnerabilities they are up against as well as their magnitude. Would the users accept and activate a virus received as an attachment via an e-mail? Would someone reply to a phishing e-mail providing important personal or corporate information? Do they understand the dangers they are up against by the exposure they have as members of the marketing department (e-mail addresses available to the public)? Do they conform with the password policies of the company? Knowing where more employees failed to live up to the expectations, they can proceed in building their defense and calibrating existing technological assets to

protect them and, more importantly, educate them and arm them against the cyber-threats they face. Not to mention that, via the evaluation process, they have already triggered them and initiated a security cultural zymosis.

Ethical and legal aspects

As with every corporate assessment tool dealing with personal data, a security culture framework reaching to an individual level needs to conform with all regional and international laws protecting human's privacy. Therefore, applications of the proposed framework need to ensure compliance with the European Data Protection Regulation (GDPR), which as of May 25th 2018, is applicable in all member states to harmonize data privacy laws across Europe.⁹⁰

Employees' evaluation results are meant to be used as a means of understanding individual security risks and training needs, discomfort from demanding and inapplicable policies, difficulties deriving from working security routine. In other words, are meant to accommodate working force by retrieving security gaps, pinpointing policy complexity and, finally, facilitating participation in cyber-security defense. They should not be considered as a rating mechanism and used as an employee competency guide since working abilities and professionalism do not always go hand-by-hand with information security awareness.²⁸ Security professionals and officers need to safeguard its role and usage, as with all security infrastructure, and to guide users through a prosperous exploitation.

Application

The directive (EU) 2016/1148 of the European Parliament and the Council of the European Union, commonly known as Network and Information Security (NIS) Directive,⁹¹ was designed to create a focus on the protection of IT systems in European critical national infrastructures (CNI). It was designed to provide legal measures to boost the overall level of cybersecurity in the EU by cultivating "*a culture of security across sectors which are vital for the economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure*",⁹² the so-called operators of essential services.

Taking into consideration the notion dictated by this recent EU legislation, the first application field targeted by the aforementioned security culture framework is the EPES sector. A business field which is trying hard to catch up technologically with the rest of the current reality and, at the same time, needs to conform to demanding security legislation. Thus, enterprises shall need to invest effort and funds to modernize their infrastructures and production cycles but, more importantly, do it in a seemingly transparent way without affecting their everyday activity. Along these lines, employees shall need to participate and be facilitated in making the transition without being discouraged by the radical and rapid changes. A holistic cyber-security culture methodology, such as the one presented in this paper, aims to assist in such cases by expediting the transition.

The first application was realized during the COVID-19 crisis via designing, developing, and conducting a tailor-made survey targeting the cyber-security culture assessment of critical infrastructures during the pandemic.⁹³ A questionnaire targeting specific security factors while bridging various security domains were designed founded on the suggested framework. Its goal was to smartly assess existing working security routine and culture, their disruption by the coronavirus crisis and their reaction to these special and rather demanding circumstances. Results revealed, among many other interesting security findings,⁹⁴ that greater emphasis is being given to corporate network perimeter enforcement whereas assets management and security is being neglected. In some cases, to a point where basic security principles are violated contradicting with the well-known security truth that "a chain is only as strong as its weakest link."

In parallel, pilot framework applications are taking place to two different European countries involving representatives from the entire electrical power and energy system supply chain, including production units, transmission system operators (TSOs), distribution system operators (DSOs), and prosumers. Targeted campaigns are designed and implemented via an iterative procedure in an attempt to evaluate the cyber-security culture of the participating employees and organizations. First results are being expected by the end of this year.

Considerations and limitations

The cyber-security culture framework presented in previous paragraphs has its foundations on a wide and diverse set of literature review. It is meant to bridge the differences and fill the gap of previously introduced tools that failed to assist managers and organizational developers in identifying what interventions to apply, why, how, and when.⁹⁵ Its holistic approach though needs to be calibrated and tested against a variety of application areas to be proven and established in the information security domain.

Multiple and flavorist case studies are needed to verify the elements (dimensions and domains) of the suggested model and, more importantly, their cohesion. Defined security controls along with their complex weighting algorithm need to be further adjusted and fine-tuned to each application environment to avoid undermining final assessment results. Finally, elaboration of the evaluation results along with participants' feedback might bring forward ideas for further assessment needs, unexploited evaluation techniques or even underestimated security facets. Time and effort need to be invested to enforce the robustness and prove the added value of the overall solution.

Conclusion and future work

Research trend appears to be moving from a technical approach of information security to a socio-cultural approach.^{53,96,97} Technical simulations and real-time testing of information systems, mathematical models, analytics, and risk assessments make room to behavioral, organizational, and criminological theories as to the basis of the cyber-security evaluation.⁴⁹

The security culture framework presented in this paper manages to combine the pros and mitigate the cons of both scientific approaches while underlining the importance of human factor in the security chain.⁹ Its iterative nature allows closely monitoring and constantly evaluating an organization's cyber-security culture which, as a living mechanism, adapts and evolves to the continuously demanding technological environment of this century.⁹⁸

Interactive evaluation methods, user appealing assessment techniques, serious gaming are only a sample of the tools encompassed in the attempt to cultivate the employee engagement and enhance security awareness on a daily basis. Personalized recommendations, fine-tuned personnel training programs, vulnerability identification and proactive initiatives result from such a fruitful security assessment. More importantly, decision-makers and actors have a better understanding of the overall organizational security readiness and are enabled to navigate their corporate technological evolution in a closely safeguarded manner.

From a methodological point of view, the next logical step is to try to correlate the resulted recognized weaknesses with the known common cyber-threats allowing for real-time simulations and risk-assessments deriving from the human factor. An even more daring challenge is to develop a correlation algorithm to automatically retrieve information from common vulnerabilities and weaknesses databases based on evaluation results and provide recommendations, training programs, or even technical solutions, if applicable. Thus, the final target being to emerge as an integral part of a security operation center (SOC) solution instead of a standalone evaluation tool.

The suggested model will be proven against different application domains and fine-tuned to comply with business needs that might have been neglected or underestimated in its weighting algorithm. But most certainly, it shall expand and evolve to constitute a core asset of a novel cyber-security philosophy; one facing the most troubling threat of all: human weaknesses.

Acknowledgments

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 832907.

Funding

This work was supported by the European Union's Horizon 2020 research and innovation program under the EnergyShield project "Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures" under Grant 832907.

ORCID

Anna Georgiadou  <http://orcid.org/0000-0002-0078-6969>
 Spiros Mouzakis  <http://orcid.org/0000-0001-9616-447X>
 Kanaris Bounas  <http://orcid.org/0000-0002-0577-2988>
 Dimitrios Askounis  <http://orcid.org/0000-0002-2618-5715>

References

1. Leeuw KD, Bergstra JA. The history of information security: A comprehensive handbook. Amsterdam (The Netherlands): Elsevier; 2007.
2. Anderson JM. Why we need a new definition of information security. *Comput Sec.* 2003;22(4):308–313, 203. doi:10.1016/S0167-4048(03)00407-3.
3. Solms BV. Information security — the third wave? *Comput Sec.* 2000;19(7):615–20. doi:10.1016/S0167-4048(00)07021-8.
4. Solms SHV. The 5 waves of information security – from Kristian Beckman to the present. In: *IFIP International Information Security Conference*, Berlin, Heidelberg. 2010.
5. Da Veiga A, Eloff JH. An information security governance framework. *Inf Syst Manage.* 2007;24(4):361–72. doi:10.1080/10580530701586136.
6. Doherty NF, Fulford H. Do information security policies reduce the incidence of security breaches: an exploratory analysis. *Inf Resour Manage J.* 2005;18:21–40.
7. Rantos K, Fysarakis K, Manifavas H. How effective is your security awareness program? An evaluation methodology. *Inf Sec J Global Perspect.* 2012 01;21:328–45.
8. Hoffman N, Klepper R. Assimilating new technologies: the role of organizational culture. *Inf Syst Manage.* 2000;17:1–7.
9. Williams P. What does security culture look like for small organizations? In: *7th Australian Information Security Management Conference*. Perth, Western Australia. 2009.
10. Business and Advisory Committee to the OECD, Securing your business. An companion for small or entrepreneurial companies to the 2002 OECD guidelines for the security of networks and information systems: Towards a culture of security. International Chamber of Commerce: OECD. 2004.
11. Smircich L. Concepts of culture and organizational analysis. *Administrative.* 1983;28(3):339–58. doi:10.2307/2392246.
12. Ouchi WG, Wilkins AL. Organizational culture. *Annu Rev Social.* 1985;11(1):457–83. doi:10.1146/annurev.so.11.080185.002325.
13. Cameron KS, Quinn RE. Diagnosing and changing organizational culture: based on the competing values framework. San Francisco (CA): John Wiley & Sons; 2011.
14. Tsui AS, Zhang Z-X, Wang H, Xin KR, Wu JB. Unpacking the relationship between CEO leadership behavior and organizational culture. *Leadersh Q.* 2006;17(2):113–37. doi:10.1016/j.leaqua.2005.12.001.
15. Harris SG. Organizational culture and individual sensemaking: a schema-based perspective. *Organ Sci.* 1994;5(3):309–21. doi:10.1287/orsc.5.3.309.
16. Lund DB. Organizational culture and job satisfaction. *J Bus Ind Marketing.* 2003;18(3):219–36. doi:10.1108/0885862031047313.
17. Herath T, Rao HR. Protection motivation and deterrence: A framework for security policy compliance in organisations. *Eur J Inf Syst.* 2009;18(2):106–25. doi:10.1057/ejis.2009.6.
18. Bulgurcu B, Cavusoglu C, Benbasat B. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. *MIS Q.* 2010;34(3):523–48. doi:10.2307/25750690.
19. Straub DW. Effective IS security: an empirical study. *Inf Syst Res.* 1990;1(3):255–76. doi:10.1287/isre.1.3.255.
20. Sharneli-Sendi A, Aghababaei-Barzegar R, Cheriet M. Taxonomy of information security risk assessment (ISRA). *Comput Sec.* 2016;57:14–30. doi:10.1016/j.cose.2015.11.001.
21. Scarfone K, Souppaya M, Cody A, Orebaugh A. Technical guide to information security testing and assessment. Computer Security Resource Center. 2008.
22. Mora M, Gelman O, Steenkamp A, Raisinghani M. Research methodologies, innovations and philosophies in software systems engineering and information systems. *IGI Global.* 2012.
23. Ronald RS. Recommended security controls for federal information systems and organizations. Special Publication (NIST SP) - 800-53 Rev 3. 2009.

24. Aurigemma S, Panko R. A composite framework for behavioral compliance with information security policies. In *45th Hawaii International Conference on Systems Sciences*, Maui, Hawaii. 2012.
25. Lebek B, Uffen J, Neumann M, Hohler B, Breiter MH. Information security awareness and behavior: a theory-based literature review. *Manage Res Rev.* 2014;37(12):1049–92. doi:10.1108/MRR-04-2013-0085.
26. Siponen M, Pahnla S, Mahmood A. Employees' adherence to information security policies: an empirical study. *Privacy Trust Complex Environ.* 2007;232:133–144.
27. Pahnla S, Siponen M, Mahmood A. Employees' behavior towards IS security policy compliance. In: *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)*. Waikoloa. 2007.
28. Workman M, Bommer WH, Straub D. Security lapses and the omission of information security measures: A threat control model and empirical test. *Comput Human Behav.* 2008;24(6):2799–816. doi:10.1016/j.chb.2008.04.005.
29. Ng B-Y, Kankanhalli A, Xu Y. Studying users' computer security behavior: A health belief perspective. *Decis Support Syst.* 2009;46(4):815–25. doi:10.1016/j.dss.2008.11.010.
30. Rhee H-S, Kim C-T, Ryu YU. Self-efficacy in information security: its influence on end users' information security practice behavior. *Comput Sec.* 2009;28(8):816–26. doi:10.1016/j.cose.2009.05.008.
31. Limayem M, Hirt SG. Force of habit and information systems usage: theory and initial validation. *J Assoc Inf Syst.* 2003;4(1):65–97. doi:10.17705/1jais.00030.
32. McCrohan KF, Engel K, Harvey JW. Influence of awareness and training on cyber security. *J Internet Commerce.* 2010;9(1):23–41. doi:10.1080/15332861.2010.487415.
33. Hu Q, Dinev T, Hart P, Cooke D. Managing employee compliance with information security policies: the critical role of top management and organizational culture. *Decis Sci.* 2012 August;43(4):615–60. doi:10.1111/j.1540-5915.2012.00361.x.
34. Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. *Comput Sec.* 2013;32:90–101. doi:10.1016/j.cose.2012.09.010.
35. Soomro ZA, Shah MH, Ahmed J. Information security management needs more holistic approach: A literature review. *Int J Inf Manage.* 2016;36(2):215–25. doi:10.1016/j.ijinfomgt.2015.11.009.
36. ISO/IEC. ISO/IEC 27002:2013(E) Information technology — security techniques — code of practice for information security controls. International Organization for Standardization (ISO). 2013.
37. ISO/IEC. ISO/IEC 27001. Information security management. International Organization for Standardization (ISO). 2015.
38. Information Systems Audit and Control Association (ISACA). COBIT5: a business framework for the governance and management of enterprise IT. 2012.
39. Eloff JH, Eloff M. Information security architecture. *Computer Fraud & Security.* 2005;2005(11):10–16. doi:10.1016/S1361-3723(05)70275-X.
- 40.. Joint Task Force Transformation Initiative. 2013. SP 800-53 Rev. 4, security and privacy controls for federal information systems and organizations. Gaithersburg (MD): National Institute of Standards and Technology.
41. ENISA. Cyber security culture in organisations. European Union Agency For Network and Information Security. 2017.
42. Petric G, Roer K. To measure security culture: A scientific approach. North America: CLTRe North America, Inc.; 2018.
43. Energy shield. [Online]. 2019 [accessed 2020 Mar 25]. <https://energy-shield.eu/>.
- 44.. CIS. 2019. CIS controls. East Greenbush (NY): Center for Internet Security, Inc.
45. All Hazards Consortium (AHC). Cyber security risk mitigation checklist. [Online]. [accessed 2019 Oct 7]. <https://www.ahcusa.org/uploads/2/1/9/8/21985670/cybersecurityriskmitigationchecklist.pdf>.
46. Utah Government. Cyber Security Controls Checklist.
47. Cybersecurity checklist series. JMARK Business Solutions.
48. ENISA. The new users' guide: how to raise information security awareness. [Online]. 2010 [accessed 2019 Oct 24]. https://www.enisa.europa.eu/publications/archive/copy_of_new-users-guide.
49. Bernik I, Prisljan K. Measuring information security performance with 10 by 10 model for holistic state evaluation. [accessed 2016 Sep 21].
50. Leach J. Improving user security behaviour. *Comput Sec.* 2003;22:685–92.
51. Furnell S, Rajendran A. Understanding the influences on information security behaviour. *Comput Fraud Secur.* 2012;2012:12–15.
52. Padayachee K. Taxonomy of compliant information security behavior. *Comput Sec.* 2012;31:673–80.
53. Ruighaver AB, Maynard SB, Chang S. Organisational security culture: extending the end-user perspective. *Comput Sec.* 2007;26:56–62.
54. Alshaikh M, Ahmad A, Maynard SB, Chang S. Towards a taxonomy of information security management practices in organisations. In: *Proceedings of the 25th Australasian Conference on Information Systems*, Auckland. 2014.
55. Chia P, Maynard S, Ruighaver A. Understanding organizational security culture. In *Sixth Pacific Asia Conference on Information Systems*, Tokyo. 2002.
56. Ngo L, Zhou W, Warren M. Understanding transition towards information security culture change. In *Proceedings of the 3rd Australian Information Security Management Conference*, Perth. 2005.
57. Vroom C, Von Solms R. Towards information security behavioural compliance. *Comput Sec.* 2004;23:191–98.
58. Andress J, Leary M. Building a practical information security program. Rockland (MA): Syngress; 2016.
59. RiskWatch. Cyber security assessment checklist. Risk Management Software Solutions.
60. ITU. Global cybersecurity index. [Online]. [accessed 2019 Oct 2]. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>.
61. Hayden L. People-centric security: transforming your enterprise security culture. New York: McGraw-Hill; 2015.
62. Da Veiga A, Eloff J. A framework and assessment instrument for information security culture. *Comput Sec.* 2010;29:196–207.
63. Munteanu A, Fotache D. Enablers of information security culture. *Procedia Econ Finance.* 2015;20:414–22.
64. Knapp KJ, Morris RF Jr, Marshall TE, Byrd TA. Information security policy: an organisational-level process model. *Comput Sec.* 2009;28:493–508.
65. Thomson KL, Von Solms R, Louw L. Cultivating an organizational information security culture. *Comput Fraud Secur.* 2006;2006:7–11.
66. Von Solms R, Von Solms B. From policies to culture. *Comput Sec.* 2004;23:275–79.
- 67.. CISCO. 2007. Measuring and evaluating an effective security culture. San Jose (CA): Cisco Systems, Inc.
68. Da Veiga A, Martins N. Improving the information security culture through monitoring and implementation actions illustrated through a case study. *Comput Sec.* 2015;49:162–76.
69. Lim J, Ahmad A, Chang S, Maynard S. Embedding information security culture emerging concerns and challenges. In *Pacific Asia Conference on Information Systems*, Taipei. 2010.
70. Lim J, Chang S, Ahmad A, Maynard S. Towards an organizational culture framework for information security practices. In: Gupta M, Walp J, Sharman R editors. Strategic and practical approaches for information security governance: technologies and applied solutions. Hershey (Pennsylvania): IGI Global; 2012. p. 296–315.
71. Safa N, Sookhak M, Von Solms R, Furnell S, Ghani N, Herawan T. Information security-conscious care behaviour formation in organizations. *Comput Sec.* 2015;53:65–78.
72. Herath T, Rao H. Encouraging information security behaviors in organizations: role of penalties, pressures and perceived effectiveness. *Decis Support Syst.* 2009;47:154–65.
73. Laycock A, Petric G, Roer K. The seven dimensions of security culture. Oslo (Norway): CLTRe AS. 2019.
74. CPNI (Centre for the Protection of National Infrastructure). Introduction to SeCuRE 4. CPNI. 2018.
75. Employee survey questions. [Online]. [accessed 2019 Oct 11]. <https://hr-survey.com/EmployeeSurveyQuestions.htm>.

76. Faily S, Furnell S, Flechais I. Designing and aligning e-Science security culture with design. *Inf Manage Comput Sec*. 2010;18:339–49.
77. Halevi T, Memon N, Lewis J, Kumaraguru P, Arora S, Dagar N, Aloul F, Chen J. Cultural and psychological factors in cyber-security. In: *18th International Conference on Information Integration and Web-based Applications and Services*, Singapore. 2016.
78. Wiley A, McCormac A, Calic D. More than the individual: examining the relationship between culture and information security awareness. *Comput Sec*. 2020;88. DOI: 10.1016/j.cose.2019.101640
79. Van Niekerk J, Von Solms R. A holistic framework for the fostering of an information security sub-culture in organizations. In *ISSA 2005 New Knowledge Today Conference*, Sandton. 2005.
80. Da Veiga A, Martins N. Defining and identifying dominant information security cultures and subcultures. *Comput Sec*. 2017;2017:72–94.
81. Da Veiga A, Martins N. Information security culture: a comparative analysis of four assessments. In: *Proceedings of the 8th European Conference on Information Management and Evaluation, ECIME 2014*, Ghent. 2014.
82. Da Veiga A. Comparing the information security culture of employees who had read the information security policy and those who had not. *Inf Comput Sec*. 2016;24:139–51.
83. CPNI (Centre for the Protection of National Infrastructure). Introduction to security. 2015.
84. SANS. Level-up test. SANS. [Online]. <https://www.sans.org/level-up/test.html>.
85. Abawajy J. User preference of cyber security awareness delivery methods. *Behav Inf Technol*. 2014;33(3):237–48. doi:10.1080/0144929X.2012.708787.
86. Saaty TL. How to make a decision: the analytic hierarchy process. *Eur J Oper Res*. 1990;48(1):9–26. doi:10.1016/0377-2217(90)90057-I.
87. Brans JP, Vincke P, Mareschal B. How to select and how to rank projects: the PROMETHEE method. *Eur J Oper Res*. 1986;24(2):228–38. doi:10.1016/0377-2217(86)90044-5.
88. Roy B, Présent M, Silhol D. A programming method for determining which Paris metro stations should be renovated. *Eur J Oper Res*. 1986;24:318–34.
89. Opricovic S, Tzeng G-H. Compromise solution by MCDM methods: A comparative analysis of VIKOR and TOPSIS. *Eur J Oper Res*. 2004;156(2):445–55. doi:10.1016/S0377-2217(03)00020-1.
90. The European Parliament and the Council of the European Union. 2018 reform of EU data protection rule. 2018 May 25. [Online]. [accessed 2020 Mar 26]. <https://gdpr-info.eu/>.
91. The European Parliament and the Council of the European Union. EUR-Lex- 32016L1148 - EN - EUR-Lex. 2016 Jun 7. [Online]. [accessed 2020 Mar 26]. <https://eur-lex.europa.eu/eli/dir/2016/1148/oj>.
92. European Commission. The directive on security of network and information systems (NIS Directive). European Commission. [Online]. [accessed 2020 Mar 26]. <https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive>.
93. Georgiadou A, Mouzakitis S, Askounis D. Towards assessing critical infrastructures' cyber-security culture during COVID-19 crisis: a tailor-made survey. In: *4th International Conference on Networks and Security (NSEC 2020)*, Sydney. 2020.
94. Georgiadou A, Mouzakitis S, Askounis D. Working from home during COVID-19 crisis – A cyber-security culture assessment survey. Mendeley Data. Athens. 2020.
95. Gathegi J, Workman MD. Observance and contravention of information security measures. In: *The 2005 International Conference on Security and Management*, Las Vegas. 2005.
96. ENISA. Cybersecurity culture guidelines: behavioural aspects of cybersecurity. European Union Agency for Network and Information Security. 2018.
97. Da Veiga A, Martins N, Eloff JHP. Information security culture-validation of an assessment instrument. *South. African Bus. Rev*. 2007;11(1):146–166.
98. Wilson M, Hash J. Building an information technology security awareness and training program. Gaithersburg (MD): National Institute of Standards and Technology; 2003:20899-8933.