World Academy of Science, Engineering and Technology
International Journal of Electrical and Computer Engineering
Vol:14, No:10, 2020

A Socio-Technical Approach to Cyber-Risk Assessment

Kitty Kioskli, Nineta Polemi

Abstract**—**Evaluating the levels of cyber-security risks within an enterprise is most important in protecting its information system, services and all its digital assets against security incidents (e.g. accidents, malicious acts, massive cyber-attacks). The existing risk assessment methodologies (e.g. eBIOS, OCTAVE, CRAMM, NIST-800) adopt a technical approach considering as attack factors only the capability, intention and target of the attacker, and not paying attention to the attacker's psychological profile and personality traits. In this paper, a socio-technical approach is proposed in cyber risk assessment, in order to achieve more realistic risk estimates by considering the personality traits of the attackers. In particular, based upon principles from investigative psychology and behavioural science, a multi-dimensional, extended, quantifiable model for an attacker's profile is developed, which becomes an additional factor in the cyber risk level calculation.

Keywords**—**Attacker, behavioural models, cyber risk assessment, cyber-security, human factors, investigative psychology, ISO27001, ISO27005.

I. Introduction

THE level of risk is assessed as a function of the impact, or consequences, of a security event (e.g. malicious incident/ act, cyber-security attack) and the probability of its occurrence. Risk assessment is a crucial process as it determines the conditions that could hamper an organization and quantify the damage that such events could cost.

Cyber risk assessment standards (e.g. ISO270x, ISO15408, ISO18045) and methodologies (e.g. OCTAVE, EBIOS, TVRA, OWASP, NIST-800, MITRE) are necessary for the secure governance of any enterprise, since cyber-attacks dramatically grow in parallel to technological innovations (e.g. IoT, AI, HPC, robotics, quantum). Cybercrime incidents reflect one of the greatest problems in society, while interrupting with daily activities, and operations, generating substantial financial losses, undermining user confidence and causing major damage to the economy and democracy [1].

All policy, technological, standardization and research efforts in risk assessment adopt a technological point of view [2]-[4]. This monolithic perspective does not consider the psychological, social or behavioural factors, although it is well acknowledged that people are the weakest link in cyber-security [5] as hackers are responsible for the cybercrimes. Thus, we need to further examine the human characteristics, understand the individual and identify his/her behaviour and psychological profile.

This paper argues that by identifying and measuring the profile of an attacker we can provide more realistic estimates to cyber-security risks. Cyber-psychology research has provided accurate profile models for attackers [6] based upon the Five Factor Theory (FFT) model [7], [8]; while the National Institute of Standards and Technology (NIST) [9] classified different attacker types according to their capability, intention and target.

In this paper principles from investigative psychology and behavioural science and risk assessment standards, such as ISO27001, 27005 [12], are applied in order to: develop a quantifiable psychological profiling model using personality, social, technical, location and motivation traits, based on Fogg's' behavioral model [10], [11]; present a socio-technical risk estimation approach that the quantified psychological profile becomes a factor in the cyber risk level calculation providing realistic estimates.

II. Related Work

This section provides the basic background principles and concepts used in the proposed socio-technical approach to risk assessment.

A. Psychological Profiles and Personality Traits

In this paper, the common definition of psychological profile is adopted, as the set of characteristics that identify the person's personality, mental and emotional stage. We use the models and theories described in this section for the development of a holistic model to classify attackers.

Psychological profiling (or just 'profiling') is broadly defined as the various techniques of identifying and analysing behaviours performed in a crime. It is mostly used in forensic psychology, but the application in cyber-security crimes appears to be feasible as well [6]. Profiling assists the investigation by either selecting the offender from a pool of suspects or by providing the offender's description for future identification [13]. A behaviour model, the B = MAT behaviour model developed by Fogg [10], seeks to identify the type of cue needed to encourage the appropriate action, dependent on an individual's motivation and ability to perform the act. According to Fogg, the likelihood of a behavior (B) occurring is a product of motivation (M), Ability (A), and the appropriate trigger (T), this is the reason is referred as the B = MAT model (Fig. 1).

Fogg's model is used to manage the behaviour which promotes defending organizations and help employees becoming more security aware and follow security practices

Dr Kitty Kioskli is a Postdoctoral Research Fellow with City, University of London, Department of Computer Science, London, United Kingdom, EC1V 0HB & Consultant at Maggioli S.p.A, Athens, Greece, 1551 24 (corresponding author, phone: +44(0)2070405060, e-mail: Aikaterini.Kioskli.2@city.ac.uk).

[14], [15]. A common *personality model* that is being used is the FFT model [7], [8], or big five personality traits, or 'the big five', introduced by McCrae & Costa [7] outlining the five traits as described in Table I.

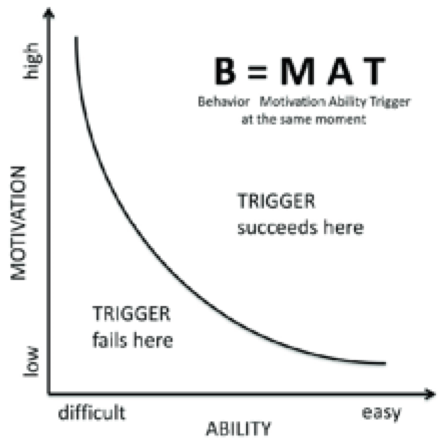

Fig. 1 The Fogg Behaviour Model [10], [11]

TABLE I
FACETS OF THE BIG FIVE PERSONALITY TRAITS [16]

Traits	Facets
Agreeableness	Trust, Altruism, Morality, Politeness
Extraversion	Gregariousness, Assertiveness/Outspokenness, Activity/Energy level, Positive Emotions/Mood
Conscientiousness	Orderliness/Neatness, Achieving-Striving/ Perseverance, Self-Discipline, Dutifulness/ Carefulness, Self-Efficacy
Neuroticism	Self-Consciousness, Vulnerability/Nervousness, Anxiety/Fearfulness, Sensitivity to tension
Openness to experiences	Intellect/Creativity, Capacity to express emotions, Imaginative, Artistic Interest/ Originality, Adventurousness

These five traits in Table I can be affected by genetic, environmental and genes' factors in combination with alternative ways of thinking [16], [17]. The above model has been used for developing hackers' personality profiles, as we will see in Section III.

B. Attacker's Behavioural Models and Psychological Profiles

Although they are various classifications of attackers (or cyber agents) found in the literature (e.g. [9], [18]), we will concentrate on the black hat hackers, who are computer criminals' representing a public threat and breach computer security for personal criminal achievement [19], [20]. The beginner black hat hacker has as a main personality trait, openness to experience while the advanced black hat hacker demonstrates extraversion, agreeableness and conscientiousness [21].

Cyber-psychology researchers have provided profile models for hackers based on personality traits, using the FFT model [6], [21]. Extended psychological profiles for hackers have been developed using not only personality factors but other factors, such as intelligence, social and technical skills [6], [9]. Finally, various cyber security threat models [22]-[24] consider hackers' classifications and basic behaviour traits in their analysis.

C. Quantification of Personality

Researchers and behavioural analysts use different approaches to measure personality and psychosocial factors (traits) of an individual. Psychological assessments provide useful data which contribute towards the understanding of a person's capabilities and characteristics [25], [26]. These data are collected and interpreted through various methods such as, rating scales [27], interviews [28] and self-reports [29].

NIST [9] adopts the *rating scale* approach and suggests a set of *attack factors* (characteristics) to describe an attacker. Types of attackers are differentiated according to their capability, intention and target (Table II). For each characteristic, a five-tier scale of qualitative and semi-quantitative values, together with a detailed description is provided.

TABLE II
DESCRIPTION OF THE HACKER CAPABILITY [9]

Characteristics of the hacker potential by NIST			
Qualitative Values	Semi-Quantitative Values		Description of the Adversary
Very High	96-100	10	Very sophisticated level of expertise
High	80-95	8	Sophisticated level of expertise
Moderate	21-79	5	Moderate resources
Low	5-20	2	Limited resources
Very Low	0-4	0	Very limited resources

Similar tables with similar attack factors have been developed (e.g. MITRE [30]) in order to capture the attackers' potential. However, none of these methodologies include psychological profiles as attack factors.

D. Theoretical Concepts of Cyber Risk Assessment

A *cyber-security threat* is defined as the potential cause of an unwanted incident (e.g. fire, unauthorized software changes), which may result in harm to a system or organization (ISO/IEC 27000:2016) [18]. Various reports annually are published indicating the most recent threat landscape [31]-[33]. The *level of a threat* depends upon the frequency of its occurrence. V*ulnerability* is defined as the weakness of a cyber-asset to be exploited by one or more threats due to lack of appropriate controls (ISO/IEC 2700x). For example, a software (asset) is vulnerable to unauthorized software change (threat) since back-up files (control) are not kept. The *level of vulnerability* (how easy becomes to overpass the control) depends upon the appropriateness of the selected controls (e.g. technical, procedural) to avoid exploiting the threat.

In case a threat is exploited (via a *cyber-attack*) it will reveal various consequences (*impact*) to the organization that owns this asset such as, financial, legal, or societal. The *impact level* depends upon the number and severity of the consequences. The *cyber-security risk* depends upon the threat, vulnerability and impact level. T calculate the cyber security risk, R_A , of a threat, T_i , to an asset A, we compute the threat level $l(T_i)$, impact level $l(I_i)$ and vulnerability level

$l(V_i)$of this threat T_i to the asset A. We continue by performing this calculation for all threats T_i that asset A faces:

$$R_A\,(T_i) = l(V_i)l(T_i)l(I_i) \tag{1}$$

By *risk assessment* we mean the above exhaustive calculation for each cyber asset, A, in our organizations' Information System, for all the threats, T_i, that each cyber asset A faces. Policy makers have issued various security policies, regulations and guidelines, such as NIS [34] and Cyber-security Act [35], to create a secure digital environment, encouraging the organizations to perform risk assessments. Standardization bodies have published various cyber-security risk assessment and management standards (ISO 27001, ISO27005), where various cyber risk assessment methodologies, implementing these standards, have been published [36]. Computer scientists have developed innovative risk assessment tools, such as CYSM [37] and Medusa [4], providing user-friendly digital tools to automate the risk assessment process.

Although the human factor is considered the most important element in cyber-security [38], in the above-mentioned risk assessment approaches, psychological factors have not been considered. With this paper, we aim to enhance existing efforts in hackers' psychological profiling and quantify hackers' psychological traits in order to more realistically estimate vulnerabilities and cyber-security risks.

III. Proposed Socio-Technical Cyber Risk Estimation Method

In this section we propose a multi-dimensional, measurable (black) hackers' profile and its personality traits based upon psychological, behavioural, societal, technical profile using the FFT personality model and Fogg's' behavioural model (Sections II *A* and *B*). A socio-technical approach to cyber risk calculation is further developed and presented.

A. Hackers' Holistic Psychological Profile

In particular, we claim that Fogg's model can be applied to hackers' behaviours. For instance, if a hacker is motivated (e.g. economic motives) to undertake an attack (e.g. Distributed Denial of Service Attack-DDoS), then addressing his ability (e.g. IT skills in using built-in terminal commands in networked machine) will increase the likelihood of carrying out the behaviour (performing an attack). Similarly, if an action is simple and the hacker is able to complete it, then addressing motivation (e.g. boredom) should also increase the likelihood. Once motivation and ability are addressed, according to Fogg's model, we should then look into triggers. These triggers, in the hackers' case, can take the form of: 1) signals (e.g. new published vulnerability), best used when the hacker is motivated and has the ability, 2) sparks that seek to motivate as well as trigger the performance of an attack (e.g. warning that computers will be at risk if the vulnerability is not treated), or 3) facilitators, that seek to both trigger a behaviour and make it easier (e.g. no control is published for this vulnerability). Therefore, we propose the following hackers' multi-dimensional psychological profile (Table III) consisting of five main traits (personality, social and technical skills, relationship, motivation) including sub-categories for each trait, utilized as measurement benchmarks.

TABLE III
Proposed Hackers' Multi-Dimensional Psychological Profile

FACETS	
Personality Traits	
Extraversion	Gregariousness, Assertiveness/Outspokenness, Activity/ Energy level, Positive Emotions/Mood
Conscientiousness	Orderliness/Neatness, Achieving-Striving/Perseverance, Self-Discipline, Dutifulness/Carefulness), Self-Efficacy
Openness to experiences	Intellect/Creativity, Imaginative, Scientifically Interested/Originality, Adventurousness
Social Traits	
Selected social exposure	Difficult to adapt to conventional social norms. Easy to build strong e-bonds with co-hackers in communities in the Deep Web. These communities are open by invitation only
Not conventional relationships	Finds social situations difficult. Easy to build professional virtual relationships. Hackers enter visual communities building strong relations and discover security vulnerabilities through social engineering, which helps them to execute sophisticated attacks
Not talkative	Difficult to initiate social talks; difficult to express him/herself in a social setting
Manipulative	Leads people into providing confidential information to compromise information systems
Technical skills & Resources	
Networking skills	Functional and operational aspects of e.g. routers and switches, DNS, HCP
IT skills	Operating Systems, languages, Software and emerging technologies
Soft skills	Problem Solver, team worker
Forensics skills	Uses security scripts, forensics tools
Available Resources	Owns or has access to high computer processing power (e.g. powerful machines, multiple Virtual Machines, HPCs) and security communities (e.g. hacking/penetration testing/cryptanalytic)
Relationship with the organization	
Insider (works in the organization), Supplier/Supply chain partner (provides services or part the organisations' value chain), Outsider	
Motivations	
Economic, political, commercial or governmental espionage, boredom, fun, revenge, evangelists of governmental openness and transparency ('us against them" view), whistle blower (warns the society of any digital wrong doings)	
Triggers	
Zero-day vulnerability warnings for attacks, price published in the Dark Web for those that will exploit the vulnerability, hackers' groups, announced that work on the exploitation of this new vulnerability	

B. Quantification of Hackers' Holistic Psychological Profile

As per the the NIST approach (Table II), for each trait in Table III, we provide a five-tier scale of qualitative and semi-quantitative values which will in turn give us a score for the profile, as described in Table IV.

In Table IV, we reveal the hackers' quantified profile which will increase the likelihood of carrying out the behaviour (performing an attack) as its value increases. This knowledge can be valuable to an organization either to identify the potential of an employee (e.g. member of security team, administrator) to become a hacker so the organization can avoid insiders' malicious attacks; or to better identify suspects after an attack during the cybercrime investigation. For example, if the organization has experienced a catastrophic attack that paralyzed the whole IT infrastructure, it can be concluded that the attacker was an expert and thus the potential suspects have the corresponding traits in Table III. These traits may serve as evidence in the cybercrime investigation, minimizing the search from a cybercriminal database.

TABLE IV
PROPOSED QUANTIFICATION OF HACKERS' PSYCHOLOGICAL PROFILE

Qualitative Values	Semi-Quantitative Values		Description of the Adversary
Very High (expert hacker)	96-100	10	Has 100% of the traits described in Table III in all categories
High (experienced hacker)	80-95	8	Has more than 80% of the traits described in Table III
Moderate (junior hacker)	21-79	5	Has more than 20% of the traits described in Table III
Low (mature hacker)	5-20	2	Has more than 5% of the traits described in Table III
Very Low (not skilled hacker)	1-4	1	Has less than 4% of the traits described in Table III

C.A Proposed Socio-Technical Method to Cyber-Risk Estimation

As we saw in Section II *D*, traditional technical risk assessment methodologies calculate the risk (R_A) of a threat T_i to an asset A, by evaluating the threat level $l(T_i)$, impact level $l(I_i)$ and vulnerability level $l(V_i)$ of this threat T_i to the asset A. We continue by performing this calculation for all threats T_i that asset A faces:

$$R_A\,(T_i) = l(V_i)l(T_i)l(I_i)\;. \tag{2}$$

The vulnerability level, $l(V_i)$, using classical methodologies, take into consideration the following four vulnerability factors (VF-i):

- VF-1: Ease of discovery which is related to how easy is to discover the vulnerability/weakness. Four possible score values can be found here: practically impossible (0), difficult (1), easy (2) and very easy (3).
- VF-2: Ease of exploit that actually depicts how easy is for an adversary to exploit the vulnerability/weakness. The score values for this factor are the following: practically impossible (0), difficult (1), easy (2) and very easy (3).
- VF-3: Ease of detection meaning how likely is for a threat to be detected. The likelihood of detection scores as follows: proactively detectable (0), actively detectable (1), post-actively detectable (2) and non-detectable (3).
- VF-4: Awareness which depicts how well-known is a vulnerability/weakness. The score values for this factor are: totally unknown (0), hidden (1), obvious (2) and publicly known (3).

Thus, the classical risk estimation in (1) based upon the four above vulnerability factors becomes:

$$R_A\,(T_i) = l(T_i)l(I_i)l(V_i){=}\,l(T_i)\;l(I_i)\;\Big(\sum_{j=1}^{4} VF_j\Big) \tag{3}$$

The authors claim that another factor needs to be considered in the risk estimation, namely factor, VF-5, where, VF-5: The average score of the profile of the potential hacker. The score values for this factor are defined in Table IV. The level of a vulnerability, $l(V_i)$, with this proposal is computed now based on five vulnerability factors, VF_j, as follows:

$$l(V_i) = VF_5\Big(\sum_{j=1}^{4} VF_j\Big) \tag{4}$$

Thus, the risk of a threat T_i to asset A becomes:

$$R'_A\,(T_i) = l(T_i)l(I_i)l(V_i){=}\,l(T_i)\;l(I_i)\;VF_5\;\Big(\sum_{j=1}^{4} VF_j\Big) \tag{5}$$

If we compare the risk estimate R_A as can be derived from any technical risk assessment calculation using (2) and the proposed new estimate, R'_A, using (4), we realise that they differ by the factor VF_5 , i.e.

$$R'_A = VF_5\;R_A \tag{6}$$

The above estimate suggests that the risk estimate is not a unique number (as treated in technical risk assessment approaches) but depends on the various profile estimates. For example, using Table III and (5), we can conclude that the advanced adversaries (expert hacker, VF-5 = 8) will increase the risk level R'_A by a factor of 8, the amateur hacker (VF-5 = 2) by a factor of 2 and the unskilled hacker (VF-5 = 1) will not increase the risk level of the traditional technical risk estimation.

IV. CONCLUSION AND FUTURE RESEARCH

In order to secure our economy and society we need to advance our cyber-security capabilities by building bridges between computer scientists, psychology researchers, behavioural scientists and sociologists to develop advanced holistic socio-technical security management and incident handling techniques. Personality profile is a main factor in psychology investigation, forensics psychology and also in cyber risk assessment (as we propose in this work). This paper reveals that the interplay between psychological investigation and behavioural findings will lead to more accurate estimation of cyber risks. By identifying personality, behavioural, social, technical, motivation and location traits, we composed a multi-dimensional psychological profile of a hacker. The quantification of the profile and its traits is leading to more accurate calculations of cyber risks. Profiling here acts as a way to have realistic estimates of cyber risks, as a proactive measure to better select employees and avoid internal attacks and as an assistance to the investigation by either select the offender from a pool of suspects or by providing the offender's description for future identification. The authors hope the work in this paper, will encourage further socio-technical cyber-security research.

ACKNOWLEDGMENT

The work in this paper has been inspired by the European

Commission H2020 project ‘A digital guardian angel enhancing cancer patient’s wellbeing and health status improvement following treatment’. The authors would like to thank the European Commission for funding this project.

References

[1] Morgan S. 2019 Official Annual Cybercrime Report, 2019 https://www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf

[2] ENISA. Inventory of risk assessment methodologies and tools, 2005 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

[3] Nikolic B, Ruzic-Dimitrijevic L. Risk Assessment of Information Technology Systems. *Issues In Informing Science And Information Technology* 2009; 6:595-615.

[4] Papastergiou S, Polemi N, Kotzanikolaou P. Design and validation of the Medusa supply chain risk assessment methodology and system. *International Journal of Critical Infrastructures* 2018; 14:1-39.

[5] Krombholz K, Hobel H, Hubel M, et al. Advanced social engineering attacks. *Journal of Information Security and Applications* 2014; 22:113-122.

[6] Lickiewicz J. Cyber Crime Psychology-Proposal of an offender psychological profile. *Problems of Forensic Sciences* 2011; 86:239-252.

[7] McCrae RR, Costa PT. Validation of the five-factor model of personality across instruments and observers. *Journal of Personality and Social Psychology* 1987; 52:81-90.

[8] McCrae RR, John OP. An introduction to the five-factor model and its applications. *Journal of Personality* 1992; 60:175-215.

[9] National Institute of Standards and Technology. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

[10] Fogg BJ. A behavior model for persuasive design. In Proceedings of the 4th international Conference on Persuasive Technology (p. 40). ACM;2009.

[11] Fogg BJ, Hreha J. Behavior Wizard: A Method for Matching Target Behaviors with Solutions. In: Ploug T., Hasle P., Oinas-Kukkonen H. (eds) Persuasive Technology. Lecture Notes in Computer Science; vol 6137. Springer, Berlin, Heidelberg; 2009.

[12] Embarking on certification to Cyber Essentials and ISO 27001. https://www.itgovernance.co.uk/iso27001-and-the-cyber-essentials-scheme

[13] Kocsis R, Hayes A, Irwin H. Investigative Experience and Accuracy in Psychological Profiling of a Violent Crime. *Journal Of Interpersonal Violence* 2002; 17:811-823.

[14] ENISA. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, 2018 https://www.thehaguesecuritydelta.com/media/com_hsd/report/228/document/WP2018-O-3-3-2-Review-of-Behavioural-Sciences-Research-in-the-Field-of-Cybersecurity.pdf

[15] Spitzner L. Public Wi-Fi Attacks,2019 https://www.sans.org/security-awareness-training/blog/public-wi-fi-attacks

[16] Pervin LA, Cervone D, John OP. Personality: Theory and research. 9-edition. USA: Wiley; 2005.

[17] Power R, Pluess M. Heritability estimates of the Big Five personality traits based on common genetic variants. *Translational Psychiatry* 2015;5: e604-e604.

[18] ISO 27005. https://www.itgovernance.co.uk/iso27005

[19] Silic M, & Lowry PB. Breaking bad in cyberspace: Understanding why and how black hat hackers manage their nerves to commit their virtual crimes. *Information Systems Frontiers* 2019; 6(1):1-13

[20] Moore R. Cybercrime: Investigating high technology computer crime. Matthew Bender and Company; 2005.

[21] Matulessy A, Humaira NH. Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits. *Psychology and Behavioral Sciences* 2016; 5:137-142.

[22] Öztürk C, Bektas M, Ayar D, et al. Association of Personality Traits and Risk of Internet Addiction in Adolescents. *Asian Nursing Research* 2015; 9:120-124.

[23] Khan, Rafiullah, et al. "STRIDE-based threat modeling for cyber-physical systems." 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe). IEEE, 2017.

[24] Sion, Laurens, et al. "Solution-aware data flow diagrams for security threat modeling." Proceedings of the 33rd Annual ACM Symposium on Applied Computing. 2018.

[25] Groth-Marnat G. Handbook of psychological assessment. Hoboken, NJ: John Wiley and Sons; 2009.

[26] Weiner IB. The assessment process. In: Weiner IB, editor. Handbook of psychology. Hoboken, NJ: John Wiley and Sons;2003.

[27] Aiken LR. Rating scales and checklists: Evaluating behavior, personality, and attitudes. Oxford, England: John Wiley and Sons;1996.

[28] Selzer MA., Kernberg P, Fibel B, et al. The personality assessment interview: Preliminary Report. *Psychiatry* 1987; 50:142-152.

[29] McCrae R. The Counterpoint of Personality Assessment: Self Reports and Observer Ratings. *Assessment* 1994; 1:159-172.

[30] MITRE Adversarial Tactics, Techniques, and Common Knowledge https://attack.mitre.org

[31] Cramm. https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html(5

[32] ENISA. Threat Landscape Reports 2013 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats and 2018 http://topintelanalysts.com/wp/wp-content/uploads/2019/02/ENISA-Threat-Landscape-Report-2018.pdf

[33] ENISA. Cybersecurity Culture Guidelines: Behavioural Aspects of Cybersecurity, 2018 https://www.thehaguesecuritydelta.com/media/com_hsd/report/228/document/WP2018-O-3-3-2-Review-of-Behavioural-Sciences-Research-in-the-Field-of-Cybersecurity.pdf

[34] The NIS Regulations. https://www.gov.uk/government/collections/nis-directive-and-nis-regulations-2018

[35] Policies on Cybersecurity-The EU cybersecurity Act. https://ec.europa.eu/digital-single-market/en/policies/75984/3587

[36] ENISA. Inventory of risk assessment methodologies and tools, 2005 https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-tools

[37] Papastergiou S, Polemi N, Karantjias A. CYSM: An Innovative Physical/Cyber Security Management System for Ports. In: Tryfonas T., Askoxylakis I. (eds) Human Aspects of Information Security, Privacy, and Trust. HAS 2015. Lecture Notes in Computer Science, vol 9190. Springer, Cham; 2015.

[38] Ani U, He H, Tiwari A. Human factor security: evaluating the cybersecurity capacity of the industrial workforce. *Journal Of Systems And Information Technology* 2019; 21:2-35.