Human Factors in Cybersecurity, Vol. 53, 2022, 138–150
https://doi.org/10.54941/ahfe1002211

Estimating Attackers' Profiles Results in More Realistic Vulnerability Severity Scores

Kitty Kioskli[1,2] and Nineta Polemi[2,3]

[1]School of Computing, Engineering and Mathematics, Centre for Secure, Intelligent and Usable Systems, University of Brighton, Brighton, United Kingdom
[2]trustilio B.V., Amsterdam, Netherlands
[3]Department of Informatics, University of Piraeus, Piraeus, Greece

ABSTRACT

The Common Vulnerability Scoring System (CVSS) is considered a standard measure for the severity of vulnerabilities. CVSS assumes that the potential attacker will be highly skilled while not considering any other human factor which may be involved. This leads to unrealistic scores that burden small companies with costly security controls. In this paper we propose that by profiling and better estimating the potential attacker in every sector, we will have more realistic and thus more accurate CVSS estimates and, consequently, affordable controls. Our paper first provides a thorough background of existing research on the synergies between cyberpsychology, psychology and behavioural principles that reveal the various traits of a holistic attacker's profile. The quantification of the profile yields the types of the attacker (basic, moderate, and sophisticated). Then, for the same vulnerability, we demonstrate how the CVSS3.1 score varies according to the type of potential attacker.

Keywords: Cybersecurity, Human factors, Attackers' profile, Vulnerabilities, CVSS, ISO2700x

INTRODUCTION

Digitalisation is moving at an increasing speed in all sectors of the economy, by 2025 the amount of stored data will grow to 175 zettabytes (HIPPA, 2018; Reinsel et al., 2018). Along with it, the cybersecurity threats and attacks continue to rise rapidly. Enterprises in all economic sectors are imposed to constantly assess the vulnerabilities (weaknesses) of their Information and Communication Systems (ICT) and estimate their severity in order to avoid their exploitability by targeted cyber-attacks.

Attacks may have catastrophic consequences (impacts) to all enterprises, including disruption or termination of operations, economic damages, long-term damaged reputation, customer loss, lawsuits, and fatalities. Organisations need to undertake mitigating actions and technical controls to lower the severity of the vulnerabilities and protect their ICT assets and data.

However, security measures are expensive, especially for small companies. Cybersecurity is considered a burden on the Small-Medium Enterprises (SMEs) and not a marketing advantage; cost is their biggest challenge

© 2022. Published by AHFE Open Access. All rights reserved.

(ENISA, 2021). We need to be as realistic as possible in our vulnerability severity scoring in order to decrease the security costs for smaller companies and further stop potential attackers from exploiting. Hence, identifying who the potential attackers for our sector and company may be is the first step to our resilience.

The classifications of attackers found in the literature are usually based on whether they are internal or external (Gaia et al., 2021) or by their means and capabilities, such as knowledge of the organization's resources, like personnel, facilities, information, equipment, networks, and systems (Chickowoski, 2018). A sector specific taxonomy was published where 15 actor types were characterized in terms of the sector, they are active in, the capabilities and the underlying motives (ENISA, 2013). Attackers are also classified according to the following traits: opportunities, means, motives and sectors or products they wish to attack (ENISA, 2021). Attack potential estimates depend upon the sector, type of attackers based on their traits. In all the above classifications, psychological, behavioural, social, and societal traits of the attackers are not considered, while adapting practical metrics to these traits is still lacking.

The existing security vulnerability measurement system is technologically and industrially driven and does not consider attackers' human traits. CVSS solely presents the assumption that the attacker is highly skilled (Kioskli & Polemi, 2020a; Kioskli & Polemi, 2020b; Kioskli & Polemi, 2020c). Even risk assessment methodologies (e.g., ENISA, 2021) used to estimate risks maintain a broad approach and do not consider the attackers' profiles. Notably, NIST and TVRA take the skills, capabilities, and motives of the attackers into account, but not all traits of their profile. Conclusively, existing security measurements or methodologies do not consider human traits in their estimates.

The aim of our work in the last years is to bridge the psychosocial advancements, including human, behavioural, and psychosocial factors, with the cybersecurity efforts to improve and reach a realistic cyber-resilient state within the information systems. More specifically, we proposed a social-technical approach in assessing the vulnerability and cybersecurity risks where the quantifiable psychological attackers' profile became a factor in the assessment (Kioskli & Polemi, 2020a). Afterwards we enhanced our approach to develop an extended profile of the attacker which can be used for estimating more accurately the attack's potential (Kioskli & Polemi, 2020b). Lastly, we considered behavioural, social, technological, and psychological traits (extending the traits in the profile) of the potential attackers as important elements of our proposed Cyber Threat Intelligence (CTI) model that makes existing cyber defense practices and estimates more realistic (Kioskli & Polemi, 2020c).

The overarching objective of the present paper is to further contribute in providing realistic vulnerability severity scoring. Our main aim is to show that the scores using the Common Vulnerability Scoring System (CVSS) will provide more accurate estimates if the attackers' profile is considered in the calculations.

This paper is structured as follows: in Section 2, a thorough review of the literature around the threat behaviour of the attackers and the priorly conducted psychological studies on this topic is offered; in Section 3, an overview of the existing efforts bridging cyberpsychology with cybersecurity is presented; Section 4 introduces the CVSS3.1 and proposes that enhanced attackers' profile in (Kioskli & Polemi, 2020c) makes the CVSS3.1 scores more realistic. The example provided in Section 4 demonstrates that the severity of any vulnerability is not unique, it depends on the ICT asset, the potential attacker in the user's environment, and their profile. We see that the CVSS3.1 score for a vulnerability increases as the attacker's profile has a higher score. Section 5 includes conclusions and recommendations for future work including practical implications, multiple interventions, and suggestions at various levels.

ATTACKERS' THREAT BEHAVIOURAL AND PSYCHOLOGICAL RESEARCH

Despite the growing interest regarding the attackers' threat behaviour and their psychological profiling the empirical evidence and results are limited (Crossler et al., 2013; Dhillon et al., 2016; Kajtazi et al., 2014; Roy Sarkar, 2010; Safa et al., 2018; Warkentin et al., 2016). This lack of studies speaks to the fact that over 70% of internal cyberattacks are not reported by the organizations (Writ, 2018) because of their concerns around security, litigation, privacy, and potential harm to their reputation (Soh et al., 2019). The paucity of data also reports to many cyberattacks remaining undetected, which does not mean that the attacked infrastructure remains unharmed. The Cybersecurity and Infrastructure Security Agency (CISA) is differentiating the organizations into the following types: "those whose members have already stolen intellectual property, and those who simply do not know it yet" and has proposed a list of potential triggers which could influence an attacker to become a threat. These characteristics are presented in Table 1, and it is worth noting that these remain unvalidated by qualitative or quantitative methods and are based on the literature and past experience.

A study conducted by Freed (2014), compared 72 cybersecurity professionals to 46 Information Technology (IT) employees and found that they differ significantly. In particular, cybersecurity specialists had higher scores of adventurousness, extraversion, assertiveness, and openness and much lower scores in self-consciousness, vulnerability, trust, agreeableness, and sympathy.

Meanwhile, the dark triad has gained increasing popularity during recent years, and it refers to a group of socially undesirable personality traits, which are interconnected but still differentiated constructs (Jonason & Webster, 2010; Paulhus et al., 2002): Machiavellianism: Manipulative, exploitive and deceitful; Narcissism: Self-centered and attention-seeking; Psychopathy: Lack of remorse, insensitive and cynical. The personality traits in the dark triad are utilized to characterize the criminal activities of the attackers and have been described as contributing variables in several cyber activities (Gaia et al., 2021).

Table 1. Characteristics of attackers at risk of becoming a threat (CISA, 2021).

Alcoholism	Lack of Social Skills
History of rules violations	Inability to get along with others
History of criminal conduct	Compulsive behaviour
Convictions	Psychopathy
History of aggression	Narcissism
Self-injury	-

In a study including 324 adolescents, it was found that cyber-aggression was correlated to psychopathy. Cyber-aggression included insulting, spreading rumours, hacking Facebook accounts, and damaging personal reputations. It was also found that narcissism and Machiavellianism were not correlated to cyber-aggression. Also, antisocial trolling has been correlated to high scores on the dark triad (Lopes & Yu, 2017). A recent study of 768 Amazon Mechanical Turk (AMT) IT employees concluded that Machiavellianism, psychopathy and narcissism were associated with sympathy for a person who uploaded salary information of higher paid employees (Maasberg et al., 2020). However, this study reported limited statistical results which reduces the generalizability and validity of them. Lastly, another study including 235 AMT IT participants explored the correlations between computer abuse, psychopathy, narcissism, and other personality variables in a survey of 200 items. In the study, emotional stability had a 0.08 association with total computer crime (r2=0.01), disinhibition had a 0.37 association with total computer crime (r2=0.14), and the association between narcissism and total computer crime was 0.26 (r2=0.07) (Seigfried-Spellar et al., 2017).

CYBERPSYCHOLOGY AND CYBERSECURITY METRICS

The human-technology interaction changes constantly in all business sectors due to digitalisation. This depends on the fundamental shifts we see every couple of years like the increased use of the Internet of Things (IoTs), social media, virtual/augmented reality (VR/AR) technologies, Artificial Intelligence (AI) and blockchain. These shifts create changes in human behaviours and perspectives.

Cyberpsychology emerges as a new and unique discipline in this digitalised era. It has been defined, in a broad way, as understanding the psychological processes and aspects involved in human behaviour while using different functions of technology (Aiken et al., 2016; Aiken, 2016; Aiken, 2019; DeMarco et al., 2017; EUROPOL, 2014). Cyberpsychology has a transdisciplinary and multidisciplinary nature which includes areas of data science, forensics, engineering, computer science, cybersecurity, and cognitive psychology. There is growing recognition and applicability of cyberpsychology by bodies like the British Psychological Society (BPS) and the American Psychological Association (APA), as well as various research activities and initiatives (Aiken et al., 2016; Aiken, 2016; Aiken, 2019; DeMarco et al., 2017;

EUROPOL, 2014). Cyberpsychology applies to all people who interact in the cyberspace (cyber users), such as innocent users and threat agents (e.g., internal, external white/black hackers). They all reveal different personality traits primarily behavioural responses, emotional functioning, perceptual processes, personality variables and addiction levels which may be associated with risky cybersecurity behaviour (EUROPOL, 2014).

As digitalisation accelerates in all economic sectors (e.g., finance, health, transport, maritime, government) and the number of cyber users rises, the technology's effects on the human psyche will continue to significantly shape both our interactions with each other, our perceptions of the world but also of the cybercrimes. Such cybercrimes are child abuse, theft, environmental damage, terrorism, physical damage, traffic manipulation, data poisoning, satellite signals spoofing, propaganda, and loss of life. Psychologists, social and behavioural scientists work continuously in the field of cyberpsychology to bring scientific knowledge and apply expertise in behaviour and mental processing related to the cyber users. Meanwhile, they also aim to shed some light to the blur that we face because of the human-machine interaction.

Regulating and policing the cyberspace (e.g., CYRENE, CYSMET, ISO/IEC 27000, NIS, GDPR) will improve the effectiveness of cyber operations and help scientists working in the cyberpsychology field. They will be able to contribute more efficiently in supporting peoples' mental health in relation to their cyber behaviour; helping enable psychological operations; facilitating intelligence operations in the cyberspace and getting more involved in hostage or ransomware situations. Providing cybersecurity standards (e.g., ISO/IEC 27000:2018; ISO/IEC 27000; ISO31000-series; NIST SP 800-37) to manage information security risks and controls of ICT in the information infrastructures also contribute towards the resilience and protection of human-machine interaction.

Previous work has concluded that the interaction between risk management and cyberpsychology improves the efforts in estimating security risks (Kioskli & Polemi, 2020a; Kioskli & Polemi, 2020b; Kioskli & Polemi, 2020c). It has also shown that the security management process and analysing the profiles of the attackers provides insights to better forecast a security threat, incident, or attack, estimates the severity of the vulnerability and manages cybersecurity risks by undertaking appropriate, cost-effective, targeted control measures. In particular, an enhanced attacker's profile has been proposed that includes the following traits as presented in Table 2:

In Table 3 the quantification of the attackers' profile is shown, revealing the various types of attackers, such as sophisticated, experienced, and moderate.

In this paper, we will extend our previous efforts by utilizing the information from Tables 2 and 3 to make the vulnerability severity scores more realistic.

REALISTIC SEVERITY OF VULNERABILITIES ESTIMATES

Among the most important traits that trigger an attacker to perform an attack is the opportunity to attack. Vulnerable (weak) assets provide the needed

Table 2. Holistic attacker profile and traits based on (Kioskli & Polemi, 2020c).

Personality	Social/Behavioural	Technical
Extraversion	Social exposure	Penetration testing
Conscientiousness	Not conventional relationships	Forensics
Openness to expertise	Not talkative	Programming
Cognition	Manipulative	Available computing power
Motivational	**Trigger**	**Soft Skills**
Political	Vulnerable assets	Attention to detail
Personal	Human errors	Not afraid to try
Social/cultural	Malfunctions	Analytical thinking
Philosophical	Maintenance problems	Problem solver

Table 3. Quantification of attackers' profiles.

Type of Attacker	Semi-Quantitative Values		Attackers' profile
Sophisticated	96–100	10	> 96% of each of the traits in each category
Experienced	80–95	8	> 80%
Moderate	21–79	5	> 21%
Basic	5–20	2	> 5%
Insufficient	1–4	0	< 5%

opportunity to the attackers. As the severity of the vulnerability increases the attacker's motive to attack the asset(s) increases respectively and the organisation needs to undertake security controls (Kure et al., 2021). Hence, estimating the severity of the vulnerabilities of the ICT assets is the main concern of all organisations, independently of their size (Suryateja, 2018). This paper supports that the type of attacker (traits of attacker's profile) vs nurture factors (sector and ICT environment) (Ridley, 2003) shape why, how, or if a malicious actor would attack an organization.

As the user's (ICT) environment is changing according to the business sector that it is active in (e.g., entertainment, finance, retail) and according to time (e.g., firewalls are reconfigured, network components are added, e-models change, newly published exploits), the types of the attackers change as well. For example, an SME in the gaming industry expects sophisticated attackers (Vaas, 2021); while the potential attacker of a Micro-Enterprise (ME) of a local fashion retailer is basic. The user's (ICT) environment in this paper is viewed as a collection of ICT assets and the potential attackers in that sector.

This section argues that by estimating the severity of the vulnerabilities adopting only a technical view not considering the potential attackers, being part of the user environment, compromises accuracy. The estimates may not be realistic, forcing the MEs to undertake unnecessary controls they cannot

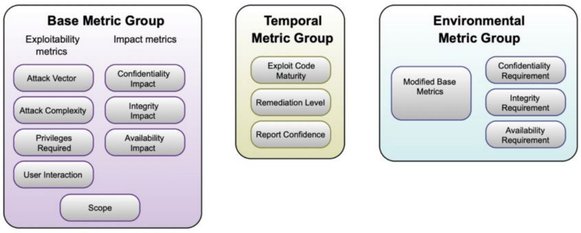

Figure 1: CVSS 3.1 metric groups.

afford, discouraging their security efforts, leaving them unprotected. Technical vulnerabilities are described by the Common Weakness Enumeration (CWE) and the severity of the technical vulnerabilities is measured by the Common Vulnerability Scoring System (CVSS). The scoring systems CVSS3.1 consists of three metric groups (see Figure 1):

- Base: Which represents the intrinsic qualities of a vulnerability that are constant over time and across ICT environments. This is the only public metric group.
- Temporal: Which reflects the characteristics of a vulnerability that is being modified over time due to various changes (e.g., new exploits are published).
- Environmental: Which represents the characteristics of a vulnerability that are unique to the ICT environment. The environment group consists of the affected assets and the implemented control on the assets (attackers are not part of the environment). It considers the effectiveness of the controls and the impacts of the vulnerability on the assets.

Each metric group has metrics that the analyst is assigning to values using the CVSS3.1 calculator. The Base metrics produce a score ranging from 0-10; it reflects the objectivity of the technical severity of the vulnerability. By providing values to the Temporal and Environmental metrics, the analyst can then modify the Base score. A CVSS3.1 score is accompanied by a vector string which, in reality, is a compressed textual representation of the values assigned by the analyst to derive the score. An example is presented at the end of this section to better depict this description.

The Environmental Metrics group applies to the vulnerability of an asset hosted in a specific environment and used for specific business purposes. This metric group relates to either the business criticality of the asset that is vulnerable, or to compensating controls or mitigations that might make the enterprise susceptible to the vulnerability. Attackers are not included in the environmental metrics (only assets and their controls) and attackers' profiles are not considered in this group. The Environmental metrics that the analyst assigns values to, are based on his knowledge and on the environment that the assets belong are: Confidentiality (CR)/Integrity (IR)/Availability Requirements (AR)/Modified Attack Vector (MAV)/Attack Complexity (MAC)/Privileges Requirements (MPR)/User Interaction (MUI)/Scope (MS)/Confidentiality (MC)/Integrity

(MI)/Availability (MA). Overall, the profiling of attackers is not considered in CVSS3.1. but solely assumes that the attacker is highly skilled.

This paper supports that if the analyst broadens the elements in the user environment, including not only ICT assets but also sectoral potential attackers then the Environmental metric group will provide more accurate estimates, enabling the analyst to customize further the CVSS score. More specifically, we propose that the analyst first identifies the potential attacker(s), the attackers' profile and then they assign values to the environmental metrics.

The Environmental metric group plays a very important role in the accuracy of the vulnerability severity estimation: if the asset is critical to the environment, the environmental score may need to be increased (if it was not considered critical in the Base calculation). If the implemented controls undertaken are effective (considering the attackers' maturity level) and the vulnerability is difficult to be exploited, then the environmental score may need to be decreased (if it was assessed higher in the Base score). Thus, as the assets' criticality change in the specific environment they belong to, then the type of attackers is also changing their profiles and maturity levels. Hence, as the effectiveness of the controls changes, the underlying attributes of the Environmental Metric will change. Consequently, by changing the environmental score, the overall CVSS score will be also adjusted.

Moreover, this paper proposes that knowledge and consideration of the attackers' profiles may influence the following two Environmental metric values:

Privileges Required (MPR): This metric describes the level of privileges an attacker must possess before successfully exploiting the asset's vulnerability. The Environmental score is higher if no privileges are required. A sophisticated attacker will not need as many privileges as the attacker with an insufficient profile to successfully exploit the vulnerability. Thus, the value assigned here will also depend upon the attacker's profile.

User Interaction (MUI): This metric captures the requirement for a human user, other than the attacker, to participate in the successful compromise of the vulnerable asset. This metric determines whether the vulnerability can be exploited solely at the will of the attacker, or whether a separate user, or user-initiated process, must participate as well. A basic attacker may not be able to exploit the vulnerability alone, but they may need a separate user to participate. While a sophisticated attacker can exploit it alone with not any user interaction. The Environmental score is higher when no user interaction is required. Thus, MUI values will also depend on the attackers' profiles.

Based on the above analysis, we propose the following scale for the Environmental values MPR and MUI for the analyst to assign depending on the potential attackers they have identified:

Example: Using the CVSS3.1 calculator for the same vulnerability, the overall CVSS score will depend upon the attackers' profile as shown in Table 4:

We realize that the score of the severity of the vulnerability decreases as the attacker's profile is less mature. The assigned values in the MPR and MUI derived from Table 5 (all other values are the same) and depend on the

Table 4. Environmental metric values based on different types of attackers.

Type of Attacker	MPR values	MUI values
Sophisticated/ Experienced	None (MPR: N) The attacker does not need to require any privileges to exploit the vulnerability.	None (MUI: N) No user interaction is needed by the attacker to exploit the vulnerability.
Moderate	Low (MPR: L) The attacker needs low privileges.	Required (MUI: R) Some interaction is needed.
Basic / Insufficient	Not Defined (MPR: X) The attacker cannot exploit the vulnerability (cannot define privileges needed).	Not Defined (MUI: X) The attacker cannot exploit the vulnerability independently of the interaction.

Table 5. CVSS3.1score varies according to the type of attacker.

	Sophisticated Attacker	Moderate Attacker	Basic Attacker
Overall CVSS3.1 score	7,9	6,7	6,3
CVSS3.1 vector string	AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:L/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:N/MUI:N/MS:C/MC:N/MI:L/MA:H	AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:L/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:L/MUI:R/MS:C/MC:N/MI:L/MA:H	AV:L/AC:H/PR:H/UI:R/S:C/C:N/I:H/A:L/CR:M/IR:M/AR:M/MAV:L/MAC:L/MPR:X/MUI:X/MS:C/MC:N/MI:L/MA:H

attackers' profile. These latter values impact the Environmental Metric and consequently the overall CVSS3.1 score.

CONCLUSIONS AND FUTURE WORK

Users (e.g., SMEs, MEs) in all economic sectors have raised cyber threat intelligence (CTI) over the years by gaining experience from past security incidents and attacks, from collaborating with their CERTs, CSIRTs, ISACs and CTI awareness activities. Their CTI level makes sectoral users to identify their sectoral and ICT environmental threats and potential attacker type. In this paper, we propose to use this knowledge (our ICT assets, sectoral threats, potential attacker type) to determine the vulnerability severity levels using the CVSS3.1 calculator more accurately.

The CVSS that was developed for enterprise information technology systems provides a standardized way of estimating the severity of a vulnerability. In this paper, we propose that the CVSS score for each vulnerability is not unique, it varies according to the type of the potential attacker. To do so we proposed that in the Environmental Metric Group of the CVSS3.1, the analyst needs to consider the attacker part of the user (ICT) environment (the original CVSS3.1 does not) when it assigns values in this metric group. Then the resulting values of the Environmental Metric Group will impact the CVSS3.1 overall score. In particular, the overall score of the vulnerability severity level decreases when the attacker becomes less mature. The more realistic scores of the vulnerabilities enable the users to select targeted controls that probably are more affordable not requiring a significant commitment of resources. This is a big challenge for small companies.

Recent claimed improvements, such as SSVC of CVSS, consider the need to involve stakeholders in the evaluation of the vulnerabilities for better decision making, however, human, psychological and behavioural factors are not considered. As indicated in this paper, cyberpsychology metrics will further improve the vulnerability scoring systems. Furthermore, it is recommended that attackers profiles shall be considered by the cybersecurity scoring systems to provide more accurate estimates for the impacts and risks estimates as well. Using attackers' profiling and the dark triad personality traits to assess new employees may be useful in the security of the organisations, to avoid internal attackers (Maasberg et al., 2020). However, it is worth mentioning that this strategy should be treated with caution for ethical, practical and privacy reasons. It is recognized that even if surveys or interviews were conducted using relevant privacy measures, such as the Dark Triad Dirty Dozen, the results would most likely be biased. This is because the individuals would probably not answer honestly in order to protect their social prestige and employment potential (Akbulut et al., 2017).

The Carnegie Mellon University Software Engineering Institute (SEI) has published a detailed guide (Householder et al., 2019) regarding tackling insiders' threats. These guidelines are thorough and include the development of control and monitoring systems, policymaking, hiring practices, addressing behavioural issues and privileged access guidelines. One of the most important points which rose through SEI is the use of positive (e.g., supporting employees) and negative (e.g., sanctions) incentives. The net result was that positive incentives might reduce security incidents and the frequency of insider misbehaviour. However, addressing insider threats remains a complex issue. It is worth noting that our proposed holistic attackers' profile traits (ENISA, 2021) can be applied to internal attackers.

Situational crime prevention and social bond theory are being utilized to address cyber threats. These theories aim to increase negative incentives towards misbehaviour and create social bonds that guide organizational security policies (Safa et al., 2018). Applying these theories and identifying other applicable ones, may facilitate an organization to develop behavioural approaches to counter cyber threats and attacks (Gaia et al., 2021).

Future work should investigate how employees and managers' profiles will also lead to a more effective selection of controls and mitigation actions, that people can accept, adopt, and practice. This would aim to strengthen the resilience of the enterprises against cybersecurity attacks. The authors continue their work in further validating the types and profiles of attackers in (Kioskli & Polemi , 2020c), in various sectors (e.g., SMEs in the gaming and health sectors); and providing more examples of the CVSS3.1 scores for various sector-specific vulnerabilities (e.g., AR/VR software used in the gaming industry).

Besides the limitations (e.g., social desirability issues) of collecting a sample of SMEs in various sectors and the potentially involved bias, this would be useful and help the research field move a step forward. With our work, we aim to help SMEs become more resilient to cybersecurity attacks and treat their vulnerabilities realistically in an affordable way utilizing the knowledge of their potential attackers. As Sun Tzu's quotes (1964) "If you know the enemy you need not fear the result of a hundred battles".

ACKNOWLEDGMENT

Funding has been received from the European Union's Horizon 2020 under grant agreement No 952690 project CYRENE and No 883273 project AI4HEALTHSEC. The authors are grateful for the financial support provided by the European Commission (EC). Special thanks to the PhD candidates Eleni-Maria Kalogeraki and Pinelopi Kyranoudi for their insights. The views expressed in this paper represent only the views of the authors and not of the EC or the partners in the above-mentioned EU projects.

REFERENCES

Aiken, M.P., Davidson, J., Amann, P. (2016). Youth Pathways into Cybercrime. Retrieved from: https://www.europol.europa.eu/publications-documents/youth-pathways-cybercrime

Aiken, M.P. (2016). The Cyber Effect. New York. Random House, Spiegel & Grau.

Aiken, M.P. Life in Cyberspace, 5th ed., Kindle edition, 2019.

Akbulut, Y., Donmez, A., & Dursun, O.O. (2017). Cyberloafing and social desirability bias among students and employees. Computers in Human Behavior, 72, 87–95.

Chickowoski, E. (2018). The 6 Worst Insider Attacks of 2018 – So Far. Retrieved from: https://www.darkreading.com/the-6-worst-insider-attacks-of-2018---so-far/d/d- id/1332183?image_number=7

Common Weakness Enumeration. Retrieved from: https://cwe.mitre.org/

Common Vulnerability Scoring System Version 3.1 Calculator. Retrieved from: https://www.first.org/cvss/calculator/3.1

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

Cybersecurity and Infrastructure Security Agency (CISA), (2021). CISA 2020 year in review. Retrieved from: https://www.cisa.gov/publication/cisa-2020-year-review

CYRENE EU H2020 project. Retrieved from: https://www.cyrene.eu

CYSMET national project. Retrieved from: https://cysmet.ubitech.eu

DeMarco, J., Cheevers, C., Davidson, J., Bogaerts, S., Pace, U., Aiken, M.P., Caretti, V., Schimmenti, A., Bifulco, A. (2017) Digital dangers and cyber-victimisation: a study of European adolescent online risky behaviour for sexual exploitation. Clinical Neuropsychiatry, 14(1), 104–112.

Dhillon, G., Samonas, S., & Etudo, U. (2016). Developing a Human Activity Model for Insider IS Security Breaches Using Action Design Research. Ict Systems Security and Privacy Protection, Sec 2016, 471, 49–61.

ENISA, (2013). ENISA Threat Landscape mid year 2013. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-mid-year-2013

ENISA, (2021). Cybersecurity for SMEs - Challenges and Recommendations. Retrieved from: https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

ENISA, (2021). Threat Landscape for Supply Chain Attacks. Retrieved from: https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks

European Parliament and Council of the European Union. Regulation (EU) 2016/679 (GDPR). Retrieved from: https://op.europa.eu/en/publication-detail/-/publication/3e485e15-11bd-11e6-ba9a-01aa75ed71a1#:~{}:text=1,Regulation%20(EU)%202016%2F679%20of%20the%20European%20Parliament%20and,)%20(Text%20with%20EEA%20relevance

EU Council Directive on Network and Information Security (NIS Directive) 2016/1148/EU. (2016). Concerning measures for a high common level of security of network and information systems across the Union. Official Journal of the European Union, L194 (19.7).

EUROPOL, (2014). Internet organized crime threat assessment. Retrieved from: https://www.europol.europa.eu> files > iocta2018

Freed, S.E. (2014). Examination of personality characteristics among cybersecurity and information technology professionals. The University of Tennessee at Chattanooga, Chattanooga, Tennessee, University of Tennessee at Chattanooga. Retrieved from: https://scholar.utc.edu/theses/127/

Gaia, J., Sanders, G. L., Sanders, S. P., Upadhyaya, S., Wang, X., & Yoo, C. W. (2021). Dark Traits and Hacking Potential. Journal of Organizational Psychology, 27(3).

HIPAA, J. (2018). Largest Healthcare Data Breaches of 2018. Retrieved from: https://www.hipaajournal.com/largest-healthcare-data-breaches-of-2018/

Householder, A., Hatleback, E., Spring J. (2019). Stakeholder Specific Vulnerability Categorisation (SSVC), Garnegie Mellon University report. Retrieved from: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=648577

IEC 31010:2019 international standard, (2021). Risk management-Risk assessment techniques. Retrieved from: https://www.iso.org/standard/72140.html.

ISO/IEC 27000-series on Information Security. Retrieved from: https://www.iso.org/news/ref2266.html

ISO Guide 73:2009, (2016). Risk management-Vocabulary. Retrieved from: https://www.iso.org/standard/44651.html, accessed on April 29 2021.

ISO 31000:2018 international standard. Risk management- Guidelines. Retrieved from: https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Jonason, P.K., & Webster, G.D. (2010). The Dirty Dozen: A Concise Measure of the Dark Triad. Psychological Assessment, 22(2), 420–432.

Kajtazi, M., Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2014). Assessing Sunk Cost Effect on Employees' Intentions to Violate Information Security Policies in Organizations. 2014 47th Hawaii International Conference on System Sciences (Hicss), 3169–3177

Kioskli, K., Polemi, N. (2020) a. A socio-technical approach to cyber risk assessment. International Journal of Electrical and Computer Engineering, 14(10), 305–309.

Kioskli, K., Polemi, N. (2020) b. Measuring psychosocial and behavioural factors improves attack potential estimates. In Proceedings of the 15th International Conference for Internet Technology and Secured Transactions, 216–219.

Kioskli, K., Polemi, N. (2020) c. A psychosocial approach to cyber threat intelligence. International Journal of Chaotic Computing, 7(1), 159–165.

Kure, H., Islam, S., Ghazanfar, M., Raza, A., & Pasha, M. (2021). Asset criticality and risk prediction for an effective cybersecurity risk management of cyber-physical system. Neural Computing And Applications.

Lopes, B., & Yu, H. (2017). Who do you troll and Why: An investigation into the relationship between the Dark Triad Personalities and online trolling behaviours towards popular and less popular Facebook profiles. Computers in Human Behavior, 77, 69–76.

Maasberg, M., Van Slyke, C., Ellis, S., & Beebe, N. (2020). The dark triad and insider threats in cyber security. Communications of the ACM, 63(12), 64–80.

Paulhus, D.L., & Williams, K.M. (2002). The Dark Triad of personality: Narcissism, Machiavellianism, and psychopathy. Journal of Research in Personality, 36(6), 556–563.

Reinsel, D., Gantz, J., Rydning, J. (2018). The Digitization of the World From Edge to Core. IDC, 27. Retrieved from: https://www.seagate.com/files/www-content/our-story/trends/files/idc-seagate- dataage-whitepaper.pdf

Ridley, M. (2003). Nature via nurture: Genes, experience and what makes us human. London: Fourth Estate

Vaas, L. (2021). Pandemic-Bored Attackers Pummeled Gaming Industry. Retrieved from: https://threatpost.com/attackers-gaming-industry/167183/

Roy Sarkar, K. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. Information Security Technical Report, 15(3), 112–133.

Safa, N.S., Maple, C., Watson, T., & Von Solms, R. (2018). Motivation and opportunity based model to reduce information security insider threats in organisations. Journal of Information Security and Applications, 40, 247–257.

Seigfried-Spellar, K.C., Villacis-Vukadinovic, N., & Lynam, D.R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. Journal of Criminal Justice, 51, 67–73.

Soh, C., Yu, S.C., Narayanan, A., Duraisamy, S., & Chen, L.H. (2019). Employee profiling via aspect- based sentiment and network for insider threats detection. Expert Systems With Applications, 135, 351–361.

Sun-tzu, Griffith, S. B. (1964). The art of war. Oxford: Clarendon Press.

Suryateja, P. (2018). Threats and Vulnerabilities of Cloud Computing A Review. International Journal Of Computer Sciences And Engineering, 6(3), 297–302.

The Directive on security of network and information systems (NIS Directive 2). Retrieved from: https://digital-strategy.ec.europa.eu/en/policies/nis-directive

Warkentin, M., Vance, A., & Johnston, A.C. (2016). Introduction to the HICSS-49 Minitrack on Innovative Behavioral IS Security and Privacy Research. Proceedings of the 49th Annual Hawaii International Conference on System Sciences (Hicss 2016), 3635–3635.

Writ, (2018). Retrieved from: https://www.ieee-security.org/TC/SPW2018/WRIT/