its personality traits based upon psychological, behavioural, societal, technical ability and personality traits using the FFT model and Fogg's behavioural model. In this paper, we enhance the characteristics that play a crucial role in adopting an attacker's behaviour, as we see in the following Table 2.

Table 2. Attackers' Characteristics

Personality Traits	**Description & Examples**
Extraversion	Gregariousness (e.g., Social engagement in attackers' groups) Assertiveness/Outspokenness (e.g., Leadership skills) Activity/Energy level (e.g., Enjoys a busy life) Positive Emotions/Mood (e.g., Happiness)
Conscientiousness	Orderliness/Neatness (e.g., Well-organized) Striving/Perseverance (e.g., Aims to achieve excellence) Self-Discipline (e.g., Persistent engagement to goals) Dutifulness/Carefulness (e.g., Strong sense of duty) Self-Efficacy (e.g., Confidence to achieve goals)
Openness to experiences	Intellect/Creativity Imaginative (e.g., Intellectual style) Scientifically Interested/Originality (e.g., Evidence-based) Adventurousness (e.g., Experiences of different things)
Cognition	Knowledge (e.g., Collecting information for the topic of interest) Expectations (e.g., Evaluating strengths and possible outcomes) Attitudes (e.g., Acting based on knowledge and expectations)
Social - Behavioural Traits	**Description & Examples**
Selected social exposure	Difficult to adapt to conventional social norms (e.g., Events) Easy to build virtual anonymous, professional relationships (e.g., Using anonymous identity has contacts with other attackers in the Deep Web) Easy to build strong e-bonds in hacking communities (e.g., These communities are closed to the public)
Not conventional relationships	Difficult to build physical relationships or contacts Easy to build professional (with other attackers) virtual, anonymous relationships under their moral code (us versus them approach)
Not talkative	Difficult to initiate small casual talks or social talks Difficult to express him/herself
Manipulative	Easy manipulating people via electronic means (e.g., phishing)
Technical Traits	**Description & Examples**
Networking skills	Knowledge in network architectures, systems, functional and operational aspects (e.g., DNS, HCP)
IT skills	Competencies in operating systems (e.g., languages, software and emerging technologies, programming)
Soft skills	Problem Solver (e.g. Understand, analyze and solve difficult problems) Social observer (e.g., Audits security behaviours)
Forensics skills	Know how to use security scripts, forensics tools (e.g., Intrusion detection/penetration tools)
Available resources	Available computing power (e.g., Owns/access to high computer processing power), devices, time, economic support security communities
Privileges	Insider (e.g., Works in the organization with significant /limited/no access) Outsider (e.g., supply chain partner with significant limited/no access) Outsider-Third party (e.g., vendor/manufacturer with indirect or
Targeted Knowledge	Information/ measurements gathered about the targets (e.g., CVSS), knowledge in effective attacks
Motivational & Social Traits	**Description & Examples**
Political	Political power (e.g., Espionage, fake news)
Personal	Personal satisfaction, feeling of accomplishment, boredom, competition, economic gain
Cultural	Whistleblower (warns of any digital wrongdoings)
Philosophical	Humanitarian/activist/ theological goals (e.g., Stealing for societal benefit)

Trigger Traits	Description & Examples
Vulnerable assets	Open ports (e.g., Zero-day vulnerability) New non-certified technologies (e.g., App, AI systems)
Human weaknesses/errors	Vulnerable infrastructures (e.g., No access control in data center) Unintentional human error (e.g., Distracted administrator) Intentional human error (e.g., Reckless but knowledge of risk)

Developing and scoring the attackers' profiles, based on the characteristics in Table 2, is a complex task since an appropriate metric system (measurements and weights) will need to be considered for each trait. A trustworthy, applicable scoring system will need to be a result from multi-disciplinary efforts between various sciences (behavioural, security, psychology, criminology, anthropology, cyberpsychology, mathematics etc.) based upon evidence-based high-quality studies and surveys. As a first attempt, to demonstrate the connection with the attacker potential we provide a general, rough scoring approach (Table 3) based upon the NIST measurements ([3]-Appendix D).

The attacker profile can be used in providing more realistic security estimates and measurements. This will be described in more details in the next section.

Table 3: Attackers' Profile

Qualitative Values	Semi-Quantitative Values		Attackers' profile
Sophisticated (multi-sectoral expert)	96-100	10	More than 96% of each of the Traits in each category in Table 2
Experienced	80-95	8	More than 80% of each of the Traits in each category in Table 2
Moderate	21-79	5	More than 21% of each of the Traits in each category in Table 2
Basic	5-20	2	More than 5% of each of the Traits in each category in Table 2
Insufficient	1-4	0	Less than 5% of the Traits in each category in Table 2

The attacker profile can be used in providing more realistic security estimates and measurements. This will be described in more details in the next section.

4. Socio-technical Security Estimates

The attackers' profiles (Table 3) will be used to estimate the attack potential, the vulnerability and risk levels. In particular, will lead us to a scoring of the attack potential (AP) following the ISO/IEC 18045 [4] values as seen in Table 4.

Table 4: Scoring Attack Potential (Ap)

AP Qualitative Values	AP quantitative values	Description
Beyond High	10	Sophisticated Profile (multi-sectoral expert)
High	8	Experienced Profile
Moderate	5	Moderate Profile
Basic	2	Basic Profile
Very Low	0	Insufficient Profile

The AP depends upon the attackers' profile. For example, an attacker with a sophisticated profile (e.g., nation-state actor, cyber-terrorist), strong motivation (e.g., commercial espionage) to attack a medical device (e.g., new insulin pump with glucose monitoring utilizing wireless communication links), who has the technical skills (e.g., hardware security) and available resources (e.g., hardware and software radio platform), we need to assume that he/she/they will be capable to develop the means to execute and succeed in attacking the medical device or develop significant offensive capabilities (AP will be Beyond High). The attacker's profile score indicates the likelihood of a person to adopt the behaviour of an attacker where the AP score indicates the likelihood of carrying out an attack.

Let us consider also the under-development health care platform ONCORELIEF (Figure 4), where patients use it to continuously monitor their health and to receive recommendations from the physician. The health data are collected in the sensing framework feeding a health application reaching the back-end database (db) where health records and medical data of the patients are stored and processed. The caregivers and doctors also provide additional medical data about the patient via the health application and a web interface. The potential of the health records to be stolen (attack) from the back end medical db (asset) will depend upon the attacker's profile enabling him to overcome the installed security controls of the platform e.g., there is a high possibility for an experienced attacker (see Tables 2, 3) to carry out the attack and steal the health records in the medical db (AP= High).

Another important security measurement is the vulnerability (weakness) level of an asset (e.g., medical db) to a specific threat (e.g., non-authorized access). The vulnerability level, $I(V_i)$, using classical methodologies, as we saw in our previous work [5,6]

take into consideration the following four (4) vulnerability factors (VFi) (see Figure 4).

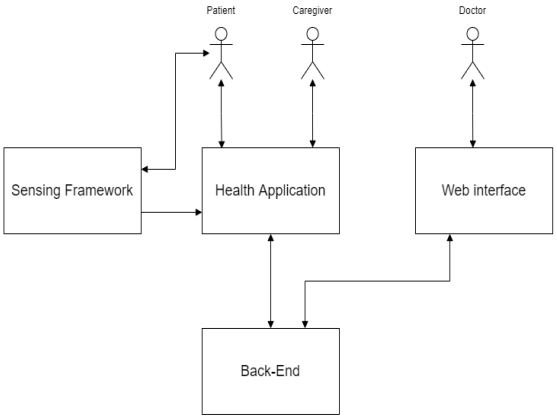

Figure 4: Oncorelief Platform [7]

- VF1: 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).

- VF2: 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).

- VF3: 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).

- VF4: 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).

The authors claimed in [5,6] that all above vulnerability factors depend upon the attackers' profile, thus the attackers' profile score needs to be considered as a new vulnerability factor namely factor, VF5. The level of a vulnerability, $l(V_i)$, was computed [5] based on five (5) vulnerability factors, VF_i, as follows:

$$l(V_i) = VF_5\left(\sum_{j=1}^{4} VF_j\right). \quad (1)$$

The above calculation led to estimate the risk of a threat T_i to an asset A as:

$$R'_A(T_i) = l(T_i)l(I_i)l(V_i) = l(T_i)\, l(I_i)\, VF_5\left(\sum_{j=1}^{4} VF_j\right), \quad (2)$$

where $l(T_i)$ notes the threat level (frequency or likehood of treat occurrence, $l(I_i)$ the impact level (consequences/damages that will reveal if a threat occurs) and $l(V_i)$ the vulnerability level of threat T_i to the asset A.

Formula 2 reveals that the risk level depends upon the attacker's profile as well. For example, the risk for the medical db (asset A) to be accessed illegally (the threat here is the non-authorized access) will depend upon the attacker's profile as well.

Another important security score is the CVSS [20] that describes the criticality of the vulnerability and depends upon the exploitability factors of the vulnerabilities; in particular, CVSS depends upon all five factors (VF1-VF5). It also depends upon the impact of the vulnerability to the standard security dimensions (confidentiality, integrity, availability). Thus, the CVSS score also depends upon the attacker's profile, VF5.

To conclude the security measurements, depend upon the attackers' profiles and thus different profiles of potential attackers indicate different security measurements. The higher the score of the attacker's profile, the higher the security measurements (attack potential, vulnerability level, risk level, CVSS).

5. Conclusions and Future Work

New emerging cybersecurity threats and attacks call to advance our CTI capabilities. The human nature, behaviour and actions make the individual the prime enabler of the cybersecurity attacks and we need to consider his/her characteristics as a crucial part of the CTI which can advance our cyber defense practices.

Considering human factors and parameters will enhance our expertise in estimating attacks' potential and cyber risks. Therefore, by considering these factors and collaborating with all experts in the relevant fields (sociology, psychology, criminology, security, behavioural sciences) will provide the necessary paradigm swift which will become so vital to boost the effectiveness of existing cyber defense methods and techniques, improve our cyber resilience and reduce cyberattack incidents.

This paper was a first attempt to quantify social characteristics and use them in security measurements to achieve more realistic security estimates. However, collaborative further research efforts are needed to enhance the methodologies (based on social sciences research instruments) that will provide appropriate metrics and measurements (qualitative and quantitative) of attackers' characteristics that will lead to more accurate attackers' quantified profiles.

Furthermore, EU security directives and initiatives (e.g., Cybersecurity Act, NIS, eIDAS) adopt solely a technical approach as well. The

authors would propose to consider a broader socio-technical view that may increase social applicability and acceptance of the security policies.

6. References

[1] ENISA (2018) 'Exploring the opportunities and limitations of current Threat Intelligence Platforms' https://www.enisa.europa.eu/publications/exploringthe-opportunities-and-limitations-of-current-threatintelligence-platforms (Access Date: 1 January, 2021).

[2] ISO/IEC 27001 (2013) 'Information technology - Security techniques - Information security management systems - Requirements' https://www.iso.org/standard/54534.html (Access Date: 20 December, 2020).

[3] National Institute of Standards and Technology (2012) 'Guide for Conducting Risk Assessments' https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (15 November, 2020).

[4] ENISA (2013) 'ENISA Threat Landscape midyear 2013' https://www.enisa.europa.eu/publications/enisa-threat-landscape-mid-year-2013 (Access Date: 15 December, 2020).

[5] K. Kioskli, N. Polemi, "A socio-technical approach to cyber risk assessment." International Journal of Electrical and Computer Engineering. 2020;14(10), pp. 305-309.

[6] K. Kioskli, N. Polemi, "Measuring psychosocial and behavioural factors improves attack potential estimates." In Proceedings of the 15th International Conference for Internet Technology and Secured Transactions. 2021, pp. 216-219.

[7] ONCORELIEF (2020) 'A digital guardian angel enhancing cancer patient's wellbeing and health status improvement following treatment' https://cordis.europa.eu/project/id/875392 (Access Date: 12 January, 2021).

[8] CC-DRIVER (2020) 'Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour A Research' https://cordis.europa.eu/project/id/883543 (Access Date: 12 January, 2021).

[9] T. Dinev, Q. Hu, "The Centrality of Awareness in the Formation of User Behavioral Intention toward Protective Information Technologies." Journal of the Association for Information Systems. 2007;8(7), pp.386-408.

[10] A. Corner, U. Hahn, "Normative theories of argumentation: Are some norms better than others?" Synthese. 2013;190(16), pp.3579-3610.

[11] A. Icek, "The theory of planned behavior". Organizational Behavior and Human Decision Processes. 1991;50 (2), pp.179-211.

[12] A. Icek, (2019) 'Theory of Planned Behavior Diagram.' http://people.umass.edu/ aizen/tpb.diag.html (13 December 2020).

[13] S. Burns, L. Roberts, "Applying the Theory of Planned Behaviour to predicting online safety behaviour." Crime Prevention and Community Safety. 2013;15(1), pp.48-64.

[14] A. Bandura, "Social foundations of thought and action: a social cognitive theory." 1986, Englewood Cliffs, N.J.: Prentice-Hall.

[15] A.B. Hardy, G. Howells, A. Bandura, N.E. Adams, "Tests of the generality of self-efficacy theory." Cognitive Therapy and Research. 1980; 4(1), pp.39-66.

[16] J. Chriss. "The Functions of The Social Bond." The Sociological Quarterly. 2007;48(4), pp.689-712.

[17] A. Matulessy, N.H. Humaira, "Hacker Personality Profiles Reviewed in Terms of the Big Five Personality Traits." Psychology and Behavioral Sciences. 2016;5(1), pp.137-142.

[18] R.R. McCrae, P.T. Costa, "Validation of the five-factor model of personality across instruments and observers." Journal of Personality and Social Psychology.1987;52(1), pp.81-90.

[19] B.J. Fogg, "A behavior model for persuasive design." In Proceedings of the 4th international Conference on Persuasive Technology. 2009; p.40.

[20] Common Vulnerability Scoring System https://www.first.org/cvss/v3-1/cvss-v31specification_r1.p df (Access Date: 20 January, 2021).

7. Acknowledgment

The research conducted in this paper was triggered by the authors' involvement in the projects OncoRelief [7] and CC-Driver [8]. The authors are grateful for the financial support of these projects that have received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreements No 875392 and No 883543 respectively. The views expressed in this paper represent only the views of the authors and not of the European Commission or the partners in the above-mentioned projects.

