Computer Standards & Interfaces 93 (2025) 103962

Contents lists available at ScienceDirect

Computer Standards & Interfaces

journal homepage: www.elsevier.com/locate/csi

Towards projection of the individualised risk assessment for the cybersecurity workforce

Agnė Brilingaitė [a,*], Linas Bukauskas [a], Ingrida Domarkienė [b], Tautvydas Rančelis [b], Laima Ambrozaitytė [b], Rūta Pirta [c], Ricardo G. Lugo [d], Benjamin J. Knox [e]

[a] Institute of Computer Science, Vilnius University, Didlaukio str. 47, Vilnius, LT- 08303, Lithuania
[b] Institute of Biomedical Sciences, Vilnius University, Santariskiu str. 2, Vilnius, LT-08661, Lithuania
[c] Institute of Information Technology, Riga Technical University, Zunda Krastmala 10, Riga, LV-1048, Latvia
[d] Faculty of Health, Welfare and Organisation, Østfold University College, B.R.A. Veien 4, Halden, NO-1757, Norway
[e] Center for Cyber and Information Security, Norwegian University of Science and Technology, Postboks 191, Gjøvik, NO-2802, Norway

ARTICLE INFO

Keywords:
Cybersecurity workforce
Individualised risk assessment
Self-regulation
Impulsivity trait
Genetic association
ICT skills

ABSTRACT

In the era of global digitalisation, there is rapid development of services requiring cybersecurity resilience against adversarial actions. The demand for skilled cybersecurity professionals is at an all-time high, with over three million positions yet to be filled worldwide. Employers call for help to recruit and retain specialists as a stressful cybersecurity work environment increases the risk of insecure and non-compliant behaviour. Current training methodologies need to be revised to address this issue, underlining the need for a shift towards more individualised training methods to raise awareness about personal traits that impact professional conduct. This paper introduces a multi-disciplinary model that enables the personal trait triangulation of the cybersecurity specialist from three different perspectives: human genetics, psychology, and information and communication technology. The model offers a novel approach by incorporating a self-regulation feature, exemplified through impulsivity measured by the Barratt Impulsiveness Scale, and leveraging a web-based system for both psychological assessment and cybersecurity task completion. Pilot experimental data (n=48) was used for model building and proof of concept. The example demonstrates model potential in individual behaviour prognosis. It suggests its utility in tailoring training strategies that not only enhance cybersecurity performance but also aid in workforce retention by acknowledging and addressing the complex interplay of factors influencing daily cyber routines.

1. Introduction

The development of new technologies enables remote maintenance of services, a rise of smart cities, an increasing reliance on automated and AI-based solutions, and the popularity of everything as a service. Therefore, technological solutions require building societal resilience against adversaries that get new possibilities to exploit newly occurring and already existing vulnerabilities. Due to these factors, the European Union Agency for Cybersecurity (ENISA) lists skill shortage and human error as emerging cybersecurity threats [1].

The extrapolated need for cybersecurity specialists has grown 350% worldwide since 2013, but the sector needs help recruiting and filling the positions [2]. Several factors for the shortage of specialists have been identified: demands for cybersecurity certifications, the increased job market for cybersecurity specialists, lack of diversity in the field, and the need for higher education and organisations to recruit, train, upskill, and retrain specialists [2,3][4, Ch. 4]. While cybersecurity workforce positions have been technology-oriented, recent industry focus and research have shown the need for a diverse workforce to ensure business continuity and solve cybersecurity incidents [3,5]. Moreover, cybersecurity-related tasks relate to a complex environment, and additional stressors arise due to staff shortages, limited budgets, and diverse attack vectors, including social engineering and insider threats [2].

While previous studies on workforce diversity have primarily focused on biodemographic variables such as gender and age, the current focus has shifted to job-related attributes [6], including educational

* Corresponding author.
E-mail addresses: agne.brilingaite@mif.vu.lt (A. Brilingaitė), linas.bukauskas@mif.vu.lt (L. Bukauskas), ingrida.domarkiene@mf.vu.lt (I. Domarkienė), tautvydas.rancelis@mf.vu.lt (T. Rančelis), laima.ambrozaityte@mf.vu.lt (L. Ambrozaitytė), ruta.pirta@rtu.lv (R. Pirta), ricardo.g.lugo@hiof.no (R.G. Lugo), benjamin.j.knox@ntnu.no (B.J. Knox).

https://doi.org/10.1016/j.csi.2024.103962
Received 14 April 2024; Received in revised form 24 September 2024; Accepted 12 December 2024
Available online 19 December 2024

background, skills, and experience. These job-related attributes help in conflict resolution on task-related issues, encourage dialogue, consolidate experience into knowledge, and foster goal achievement, all leading to creative problem-solving [6]. Within the cybersecurity domain, while there are limited studies on the effects of workforce diversity on cybersecurity operations, the following character traits have been identified and recommended for cybersecurity specialists: systemic thinkers, team players, motivation for continued learning, strong communication ability, a sense of civic duty, and a blend of technical and social skills [7].

The vital elements of the cybersecurity work environment and required skills have their basis in psychological processes related to the development of metacognitive skills, including self-regulative ones. Self-regulation as a characteristic has been validated and predicts successful outcomes in many domains [8]. However, research within the domain of cybersecurity is lacking [9]. In particular, the need to integrate Human factors research into cybersecurity specialist training has been highlighted, as often the focus is too much on the use of technology to combat threats [10]. Research has shown that mental agility is required to succeed in the cyber domain [11]. This insight entails understanding to the level of being able to manipulate physical, software, and human components [7].

Human factors usually have two forming forces: environmental and natural (predisposed by genes). Various studies have shown that almost all traits and behaviours are at least partly influenced by genetic factors [12]. Modern genomics advances offer new possibilities and applications. Because self-regulation/ self-control is a powerful predictor of health, wealth, and public safety [13], numerous studies examine why self-control differs among individuals. Genome-wide profiles of trait predictory markers could be an empowering tool by helping individuals understand their strengths and potential challenges and act accordingly afterwards. Sociogenomics findings can improve our understanding of not only the genomic and biological factors but also familial and social factors that combine across the life course to affect educational outcomes. Incorporation and uptake of genomic data may help improve policymaking and the design of actual education interventions [14]. Yet, the success of interventions and their acceptance in society depends on the ethical behaviour of stakeholders because the improper attitude towards genetic research may lead to a discriminative and vulnerable environment for some population groups [15].

This paper aims to propose a multidisciplinary model and demonstrate proof of concept (PoC) as a basis towards the individualised risk assessment of the cybersecurity workforce. The work combines human genomics, psychology, and computer science research to develop an applicable solution, PoC, to support modern staff training considering individual human traits. To our knowledge, no existing research combined the three disciplines mentioned above and executed experiments with a target group of cybersecurity specialists and a control group. We fill the existing research gap in the cybersecurity field by analysing behavioural characteristics such as self-regulation, which are vital in the daily routines of specialists. The work aims to assess the feasibility of self-regulation initially from multiple directions when applied to the cybersecurity workforce. The state-of-the-art experimentation involved a web-based prototype to collect self-reported traits and assess skills related to information and communications technology (ICT). We executed the experimental analysis to demonstrate the PoC and promote the trait research possibilities to support global efforts to retain and recruit the cyber workforce.

We hypothesise that there are features, such as self-regulation/ self-control, which might be the critical elements for a cybersecurity specialist's successful work and which could be advanced, at least to some extent. To justify this hypothesis, we formulate the following research questions:

RQ1 What are the typical self-regulation-related parameters of cybersecurity specialists compared to the general population?

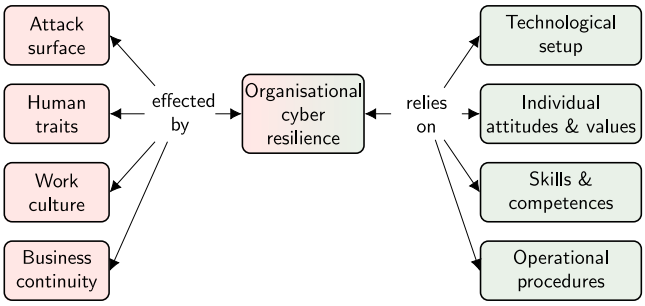


Fig. 1. Factors impacting organisational cyber resilience.

RQ2 What self-reported individual preferences, e.g., decision-making or planning styles, related to everyday activities are common to cybersecurity specialists?

RQ3 How could the interdisciplinary approach into the cybersecurity workforce development help provide recommendations to advance the work of cybersecurity specialists?

The remaining parts of the paper are structured as follows. In Section 2, we provide the background information defining the workplace specifics of the cybersecurity field and how it is bound to one's metacognitive abilities and self-regulation, which, in part, are determined by genes. Section 3 refers to the methods used to answer research questions and the primary hypothesis. Section 4 provides the extraction of the results. Section 5 discusses the results' implications from both theoretical and practical perspectives, including study limitations and ethical aspects. Section 6 concludes with our study's findings, insights, and future prospects.

2. Background

This section reviews the background research to highlight the importance of a multidisciplinary approach in developing a resilient CS workforce. Applying good modelling practices, we created three conceptual models (Figs. 1–3) to accompany each subsection and systemise the dominant interrelated concepts identified in the literature and related to our study.

2.1. Context of the cybersecurity workplace

The existing cybersecurity skill and role frameworks define the working environment of the specialists and work as a standard when the global, regional, national, and organisational needs regarding workforce development are determined. The National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework [16] distinguishes more than 50 work roles and defines the associated skills, abilities, and tasks. The European Cybersecurity Skills Framework (ECSF) [17] defines 12 roles and associates them with main tasks and key skills, including e-competences and their levels according to the European e-Competence Framework. The cybersecurity workforce deals with protecting compound systems (services, networks, devices, programs, and humans) from digital attacks. Typically, there are several responsibility areas [16]. For example, the *Oversee and Govern* area includes management and advocacy to ensure efficient work of an organisation, *Operate and Maintain* means satisfactory system performance every day, and *Protect and Defend* involves incident response and crisis management. Thus, building cybersecurity capability means establishing a resilient environment to ensure business continuity and fast response to incidents by creating (cyber)security culture and procedures, choosing proper technological tools, and training staff to succeed in decision-making processes and adapt to changes or needs.

Fig. 1 lists vital factors having an impact on organisational resilience. A timely response to an incident relies on adequately chosen and applied technological tools, the joint competence set of the recruited staff, defined operational procedures, and the attitudes and values of the individual employees. Risks to resilience come from the changing attack surface, missing elements of the work culture, requirements to ensure business continuity, and personal traits of employees. This subsection discusses the listed factors that define the context of the cybersecurity workforce.

Various work roles execute cybersecurity operations and processes [16,17]. The complexity of cybersecurity tasks requires effective collaboration between cybersecurity specialists and related technology, compliance, and management roles. The specialists have to support legacy systems, the Internet of Things, stand-alone software solutions, and heterogeneous or distributed systems, including products of a third party. This technological width makes an attack surface diverse and complex, with vulnerabilities in operating systems, open-source libraries, and software of global vendors. Thus, organisations, especially the bigger ones, with a high maturity cover several typical specialist roles to build resilience against adversaries. For example, a Chief Information Security Officer (CISO) manages an organisation's cybersecurity strategy; a Cyber Incident Responder monitors the cybersecurity state and manages incidents; and a Cybersecurity Architect designs solutions through security by design [17].

Meanwhile, the dynamic and uncertain environment of cybersecurity operations requires fast and non-impulsive decision-making and impartial problem and conflict resolution. The organisation's management Board assumes the CISO is responsible for a data breach and other incidents, leading to continuous stress at work [18]. By choosing a proper communication strategy, the CISO can reduce work stress [19]. Human error is one of the threats [1], and end users are also an exploitable vulnerability [7]. Georgiadou et al. [20] present a cybersecurity culture framework to evaluate an insider threat that arises due to the human factor being present. For example, personality predispositions might lead to espionage, sabotage, and unintentional actions because of a high-stress level. Aigbefo et al. [21] emphasise that habit and hardiness personality traits (commitment, challenge, and control) help to stay involved in security problem-solving and communication tasks under the pressure of stressful conditions. Employees can develop them to comply with security. Rational decision-making significantly affected device securement and proactive awareness [22]. Moreover, perseverance (hardiness) is seen as a vital trait in dealing with continuous stressors or challenges that require a sustained response, e.g. regular backup [23]. Thus, this characteristic is part of individual resilience against threats.

Therefore, cybersecurity work roles are expected to have a balanced set of technical, operational, and general competences [24]. For example, cybersecurity advocates [25] have to be technical enough but also possess soft skills and characteristics like communication abilities and patience to help others increase security awareness. Robinson [26] even suggests that human factors engineering could help deal with challenges arising from human factors of general users and professionals, for example, by early indication of alert fatigue of Security Operation Centre professionals. When employees work under time pressure, psychological constructs lead to disregarding security warnings or looking for non-secure workarounds [27].

Employers search for diverse skills, and Graham and Lu [28] identify that the diversity of skills is closely related to soft skills like organisational, communication, and problem-solving skills. Critical and strategic thinking, team collaboration and communication, problem-solving, and working under pressure are typical general competences associated with cybersecurity specialists [29–31]. Personality traits like self-regulation, self-control, emotional stability [32], and risk adversity [33] tend to impact human cybersecurity behaviour. Steinke et al. [34] provide recommendations to improve the performance of cybersecurity incident response teams (CSIRTs). For example, training sessions such as perturbation and stress exposure for *team adaptation* would prepare specialists to maintain adequate performance in cyber crises, and efforts to strengthen *problem-solving skills* would develop *thought habits* required during cyber incident management. Enhancing *team communication* and developing *shared knowledge*, i.e., *mental models*, are also crucial. Self-control might reduce the individual's (end-users and specialists) engagement in vulnerability-rising practices [35]. Hence, it is vital to consider behavioural aspects in the cybersecurity specialist selection, training, and management.

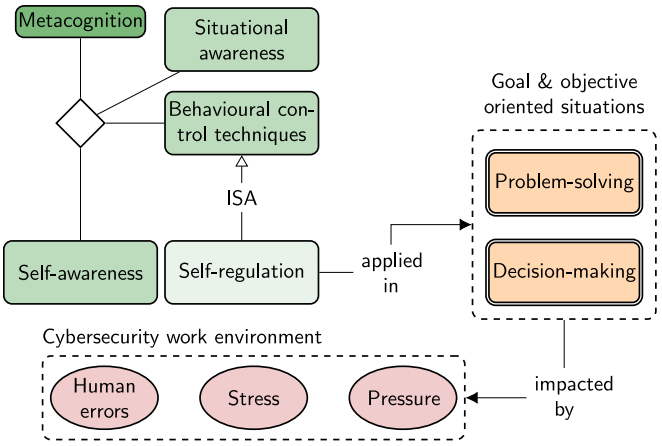


Fig. 2. Self-regulation characteristic in building cyber resilience.

2.2. Self-regulation as part of metacognition

The existing cybersecurity role descriptions [16,17] presented above have their basis in psychological processes that require the cybersecurity workforce to have self-regulatory skills.

Flavell [36] initially defined metacognition as comprising four elements: knowledge, experience, goals, and strategies. However, subsequent human factors research has expanded this concept to encompass a broader and more dynamic understanding. The awareness of one's own knowledge, experiences, and skills, along with the ability to comprehend, regulate, and manipulate cognitive processes. For instance, Suss and Ward [37] highlight the necessity for individuals to demonstrate metacognitive skills by knowing when to trust their intuitions and when to adaptively replan based on situational complexities and the consistency of their expectations. Furthermore, the concept of situational awareness, as part of the Comprehensive Information Security Awareness (CISA) framework, involves integrating security, system, and situational awareness into training through various artifacts like tutorials, case studies, simulations, and visual aids [38]. This newer understanding integrates Flavell's foundational framework with contemporary insights, reflecting a more comprehensive view of how individuals monitor and adjust their cognitive functions to effectively manage complex and dynamic situations.

Fig. 2 provides a high-level illustration explaining self-regulation's application in the cybersecurity work environment. In the figure, rectangular shapes with rounded corners represent metacognitive knowledge elements. Metacognition is an aggregate (visualised by a diamond) of three components, i.e., situational awareness, self-awareness, and behavioural control techniques. Furthermore, nodes with a double border distinguish processes and skills required in situations oriented towards goals and objectives. Ellipses demonstrate negative factors in the cybersecurity work environment. Self-regulation is a behavioural control technique vital in cybersecurity incident management. In the figure, the relationship ISA emphasises the specialisation of behavioural strategies. This notation will also be used in later figures. Factors such as stress, pressure, and human errors impact decision-making

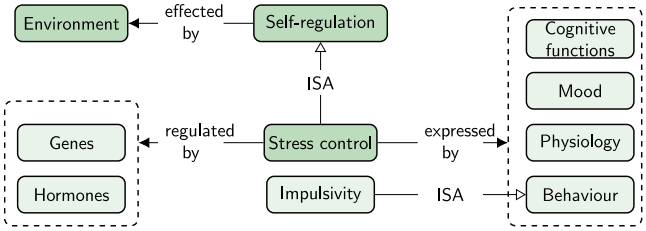


Fig. 3. Deconstructing stress control as part of self-regulation.

and problem-solving in cybersecurity work environments. Therefore, specialists should be able to control emotions and behaviour to ensure organisational cyber resilience.

Self-regulation can be understood as an interaction between personal, behavioural and environmental processes [39]. In particular, these processes are adapted in order to attain a particular goal. Whilst metacognition plays a role in these processes, self-regulation is also affected by self-efficacy, the belief one has in one's ability to achieve a particular goal [40, p. 14]. The process of self-regulation includes setting goals, monitoring goal progress, and acting in accordance with the goal [41,42]. It has been argued that self-regulation involves the following three processes: (1) behavioural self-regulation, involving observing and adjusting one's own learning; (2) environmental self-regulation, which involves observing and adjusting environmental conditions or outcomes; and (3) covert self-regulation which involves monitoring and adjusting cognitive and affective states [40, p. 15]. Whilst self-regulation is considered a fairly stable individual trait, it can be developed, for example, through modelling and/or mentoring and through personal effort [11]. To promote better self-regulation, interventions can be focused on behavioural (i.e., goal setting, impulse control), cognitive (i.e., decision-making, perspective-taking), or emotional skills (i.e., coping strategies, emotion-regulation; [43]).

2.3. Genetics underlying self-regulation

Self-regulation is a feature in part determined by genes, which makes studying it demanding because both genetic and environmental factors are involved [44]. Unlike the monogenic inheritance pattern, where a single genome variant could influence a particular trait (or disease), the multifactorial inheritance pattern (as in the self-regulation case) involving many genome variants provides only a propensity for an individual to develop a particular trait or disease. However, some genome variants may have more significant effects than others, and in behaviour cases, these variants can alter genes related to hormones [45] or other metabolic counterparts [46].

It is known, that multiple hormones affect social behaviour (could be also extended to cybersecurity behaviours as these are still behaviours in general), as often they directly influence some aspect of brain function. Hormones are not only regulated by genes. They also change gene expression or cellular function and affect behaviour by increasing the likelihood that specific behaviours occur in the presence of precise stimuli [45]. Hormones are produced by particular groups of cells called endocrine glands (pituitary, pineal, thymus, thyroid, adrenal glands, the pancreas, and the testes in men and the ovaries in women) and influence human physiology [47], which may affect behaviour [48]. The following example shows the whole cascade of processes.

Fig. 3 provides a high-level diagram that complements the example. It illustrates how stress control, as a sub-process of self-regulation, is influenced by genes and hormones. The environment influences self-regulation. In the figure, stress control is deconstructed to impulsivity, one of the behavioural patterns (ISA relationship). Stress is expressed as changes in mood, physiology, behaviour, and cognitive functions.

The vital need for self-regulation to deal with stress is a part of a cybersecurity operator's everyday working experience. Research has shown that the cybersecurity workforce operates under stress, and almost 47% of incident responders have experienced burnout or extreme stress [2]. In the body, environmental stress is transformed into cellular stress signals through biological pathways [49]. Between the environment and cells, there are regulatory elements—hormones. Hormones are released as a result of biochemical reactions orchestrated by the genome factors. The stress pathway in an organism is driven by hormones such as corticotropin-releasing hormone (CRH; impacts the body's response to stress), adrenocorticotropic hormone (ACTH; released after CRH stimulation and impacts release of cortisol and androgens) or cortisol (primary stress hormone). But it also changes/affects dopamine [50], serotonin [51], and noradrenaline [52]. Dopamine is associated with mental health, serotonin controls the mood, and noradrenaline plays a significant role in regulating attention, cognitive functions, and stress reactions. Dopaminergic and serotonergic neurotransmitters have been extensively studied in relation to self-regulation [53]. Genetic influence on self-regulation can also manifest itself in non-direct aspects of physiology, e.g., the serotonin transporter gene variant was found to be associated with lower respiratory sinus arrhythmia/ vagal tone [54]. Research on the stomach hormone *ghrelin* showed how impulsiveness, i.e., lack of self-regulation, could depend on hormones. Through gut-brain signalling, this appetite-stimulating hormone can induce impulsive behaviour [55], both motor and choice.

It was shown that there are gender differences in self-regulation-related behaviour. Age, health, and even household status were found to interact with gender and, eventually, patterns of self-regulation [56]. Gender differences could also be due to hormone differences. Women with high levels of oestrogen (in the fertile phase of the menstrual cycle) tend to be less impulsive, i.e., have higher self-regulation than men [57]. Moreover, it was demonstrated that testosterone was also linked to self-regulation, e.g., a father's ability to exert self-control moderates the link between their testosterone levels and parenting quality [58].

Meta-analysis has shown a high probability of self-control heritability (60%), indicating that genes significantly contribute to the interindividual variation of self-control and should be considered whenever analysing this trait [13].

3. Methods

3.1. Model development

We propose a three-layer multi-perspective model that enables investigation of the behaviour, health, and knowledge to create a multifaceted view of the specialist profile. The profile would work as a baseline for individual risk management and training recommendations. Fig. 4 shows the overall schematics of the suggested model. Field specialists such as educators, psychologists, and various stakeholders are involved in providing testing tools and interpretation schemas.

The first layer relates to biomedical data collection and human genetics. Genomic data, especially if combined with other data relating to an individual, can reveal behavioural traits and predispositions held by the cybersecurity specialist. It does not necessarily imply a specialist has a particular trait but rather a predisposition, where environmental conditions are also fundamental. For example, several genetic studies directly focus on self-regulation and related behaviour, such as impulsivity, aggression, addictions, sensation seeking and vigilance. A high amount of data in these studies is obtained from genome-wide association studies (GWAS) that provide hundreds of genome variants related to this behaviour [59–62]. Linnér et al. [62] studied the genetics of self-regulation by analysing 1.5 million people's genomic data. They identified more than 500 genetic loci related to it. A high number of genetic loci for self-regulation means that thousands of genome variants (with mild effect) add to self-regulation behaviour. Thus, the

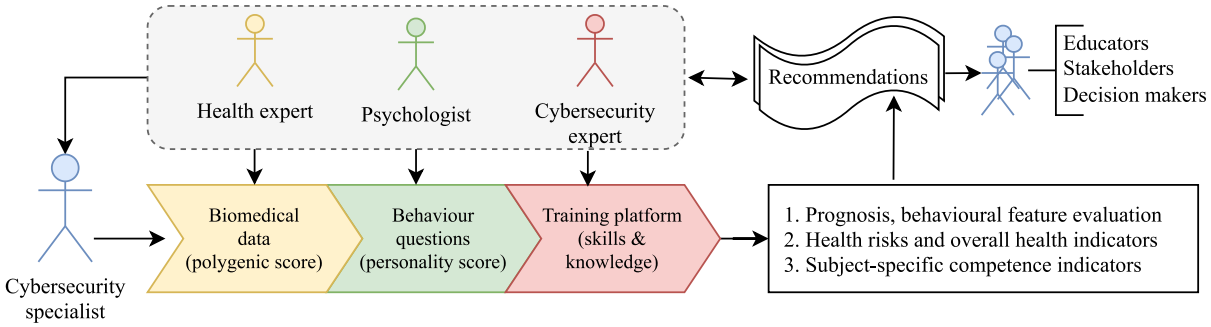


Fig. 4. An abstraction of the suggested three-layer model.

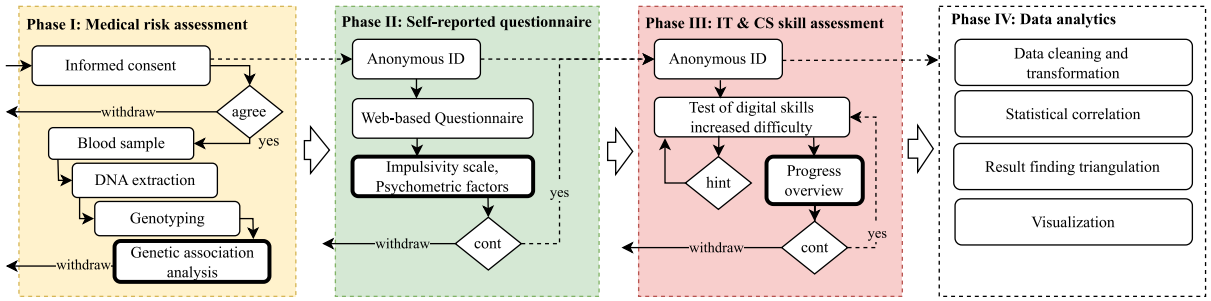


Fig. 5. The schematic overview of the experimental protocol.

layer includes blood sampling followed by DNA extraction and genetic association analysis.

The second layer is associated with self-reporting of psychological characteristics. For example, the self-control scale is described by several components like impulsivity and risk-taking [63]. Ifinedo [64] concluded that employees with high self-control were more likely to avoid risky behaviours; thus, specific training should be provided for individuals with low self-control. Building good cybersecurity habits is vital, and training could ensure behavioural comprehensiveness that positively impacts cyber habits, as shown by Hong and Furnell [65]. In our proposed model, the psychologists provide validated questionnaires and gamified tools to obtain personality scores related to the required characteristics, such as self-control, risk-taking, and addiction, to help build individual self-awareness.

The third layer provides the digital training environment to assess specialist skills and knowledge where the trainee makes some motoric action to go through the designed scenario. The behaviour component considers impulsivity as one of the self-regulation properties, as previous research identified that attentional and motor impulsivity were predictors of risky behaviours [66]. Previous research found a positive association between impulsivity control and security intentions [67]. Nevertheless, proactive awareness correlates with behavioural control and password generation [68]. Planned behaviour positively correlates with an attitude to updating regularity. At the same time, demographic parameters like age, education, and gender are not significant factors for secure behaviour [68]. Moreover, Aivazpour and Rao [69] discussed that threat risk is more associated with motor impulsiveness (physical acts) than attentional impulsiveness (concentration), e.g. information disclosure, in the online environment. Thus, the digital specialist training component includes tasks requiring attention, motoric efforts, and other features to identify trainees' behaviour under the developed plan.

The proposed three-layer model architecture supports researchers, educators, stakeholders, and decision-makers with behavioural, health-related and competence-based indicators by automatically scoring results and constructing individualised training recommendations.

3.2. Study design

The research team built a prototype of the proposed model as a PoC and executed the experiment. Fig. 5 provides an overview of the experiment phases and a protocol. The research team set up the whole experiment in four major phases, with an option to withdraw at any time, and guaranteed the anonymity of the experiment participants.

The first phase (Phase I) was dedicated to biomedical data acquisition. The first part of the phase was concluded at the medical facilities to guarantee certified blood sampling. The other parts dealt with DNA extraction, genome-wide genotyping, and genetic association analysis. During this phase, written informed consent was obtained from all of the study participants. Volunteers were provided anonymous and randomised identities and passwords to use in later phases. Solid rounded boxes identify the process that delivers volunteers a digitised version of the results. In this paper, we chose to perform genetic association analysis on the selected samples to demonstrate the PoC's interdisciplinary approach. We selected one genetic variant, rs6872863, in gene *ELOVL7*, associated with self-regulation impulsiveness identified by the Barratt Impulsiveness Scale (BIS-11) [70]. We compared the cybersecurity specialists (target) group and control group allele frequencies of the variant rs6872863 (actual genetic variant nomenclature NC_000005.10:g.60792321T). Allele is one of the two possible (in our case, it is *T* or C, C being the variant allele associated with the trait) versions of DNA sequence at the same position (DNA nucleotide sequence number 60792321).

During the second phase (Phase II), the participant logged in to a web-based system. The system provided a specific set of psychological inventories as a complete questionnaire. Additionally, participants answered demographic questions such as age, education level, gender, work role (if it is cybersecurity-related), and IT-relatedness. The system handled the questionnaire as a tool for self-reporting and automatically generated the summary of results. Notably, this work only discusses the validated Lithuanian (translated) version of the BIS-11 [70–72] inventory used in the questionnaire (provided as supplemental material in Appendix B). The BIS-11 30-item self-reported questionnaire scores a total impulsivity score, three second-order factors, and six first-order factors, e.g. self-control, perseverance, and attention. Therefore,

the BIS-11 inventory supports research questions because aggregated factors relate to question RQ1 about self-regulation-related parameters, and participants self-report individual features (required in RQ2) in the 30-item questionnaire with a 4-point Likert scale, e.g., items about planning, liking puzzles, attention during lectures, and boredom. The web-based system collected and stored data in the relational database management system. The back-end system supported the necessary database functions to get participant scores and a description of the result interpretation. Each participant received a report of questionnaire results, including calculated assessments and their meanings.

The next phase (Phase III) started when the participant entered the Capture The Flag (CTF) environment to answer questions, solve tasks, puzzles, and cybersecurity and ICT-related challenges of various types. The system integrated the CTF as a component. Note that another component of the system was the psychological questionnaire. In the experiment, the CTF included two sets of challenges: cyber hygiene questions to demonstrate skills, e.g., defining proper Wi-Fi usage, and highly technical questions, e.g., identifying network protocols in the PCAP snippets. In the scenario, more difficult questions were available only after the participant finished the tasks requiring less effort. The specialists could also do cyber hygiene tasks, and the control group could try ICT challenges. In some challenges, the participants could use the hint system. A participant could stop and consider complete withdrawal at any time.

The purpose of the last experiment's phase (Phase IV) was to qualitatively and quantitatively analyse the results of multiple participants. The research team performed data cleaning and transformation, applied tools to analyse the data and make triangulations, and visualised results to make the conclusions for the initial results. Phase IV allowed the team to answer research question RQ3 about the multidisciplinary prognosis for the individual and identify its limitations.

3.3. Data collection

The study and experiments were conducted according to the established ethical guidelines of the Code of Academic Ethics and Regulations of the Academic Ethics Commission of the Core Academic Units of Vilnius University. In compliance with applicable international and local legislation (including GDPR and the Republic of Lithuania Law On Ethics of Biomedical Research), permission No. 2022/4-1417895 of the Vilnius Regional Bioethics Committee had been received to perform this study. The collected data over a period of time and the management of biological and digital derivatives were agreed upon in the research project's data management plan, which was approved by the Research Council of Lithuania. The invitation to participate in the research was announced publicly on social media and Vilnius University web pages. All the participants of the experiments were introduced to the research procedure. They had the option to retract from the experiment at any time, with the option to request the deletion of personal data and the extraction of biological data. The announcements and questionnaires were prepared in Lithuanian to recruit local participants as defined in the application for permission from the Bioethics Committee. The participants contacted the researchers voluntarily and signed informed consent. As a reward, they were provided with feedback on psychological inventory results (after the questionnaire completion) as well as the report on *MTHFR* gene variant rs1801133, known for its importance in homocysteine levels, thrombophilia, cardiovascular function, and other phenotypes [73].

Data collection was organised as a sequential process according to the phases applicable to each individual (see Fig. 5) with the guaranteed single-directional data flow. Random non-identifiable unique keys and passwords were used to link digitised and anonymised versions of genome data. For genome data generation purposes we extracted DNA from a peripheral venous blood sample (Qiagen Puregene® DNA kit extraction protocol from blood) and performed genome-wide genotyping using Illumina microarrays (InfiniumOmni5Exome-4v1.3, Illumina Inc., USA). Genotyping data was analysed using dedicated Illumina software GenomeStudio v2.0. All samples passed the QC parameters following the manufacturer protocol recommendations.

Only digital aggregates from the first phase were merged during data analysis with data from the second and third phases. The data in web-friendly formats (JSON) and recorded action logs (.log) have been converted into an analytical ready form and stored in a relational PostgreSQL database. The research team created a set of stored PL/pgSQL procedures on the back-end to support a visual individual report generated on the front-end. The data were transformed and made ready for analytical tools with necessary meta-data.

Table 1
Demographic information.

	Cg	CS
Gender (M/F/O)	10/15/0	20/3/0
Age (mean)	35.3	29.7
Age (median/SD)	34/6.54	30/4.88
Occupation (Work/Study/Work&study	25/0/0	20/0/3
IT-related	4 (out of 25)	21 (out of 23)
Education (iC/C/iBSc/BSc)	0/2/0/4 (24%)	2/6/1/4 (57%)
Education (iMSc/MSc/PhDc/PhD)	0/11/1/7 (76%)	5/5/0/0 (43%)

Notations.
Cg—control group, CS—target cybersecurity specialist group.
Gender: M—male, F—Female, O—other.
Education: iC—incomplete college education, C—college education, iBSc—incomplete bachelor level education, BSc—holding university bachelor degree, iMSc—incomplete master studies, MSc—holding university master degree, PhDc—incomplete doctoral studies, PhD—holding PhD degree.

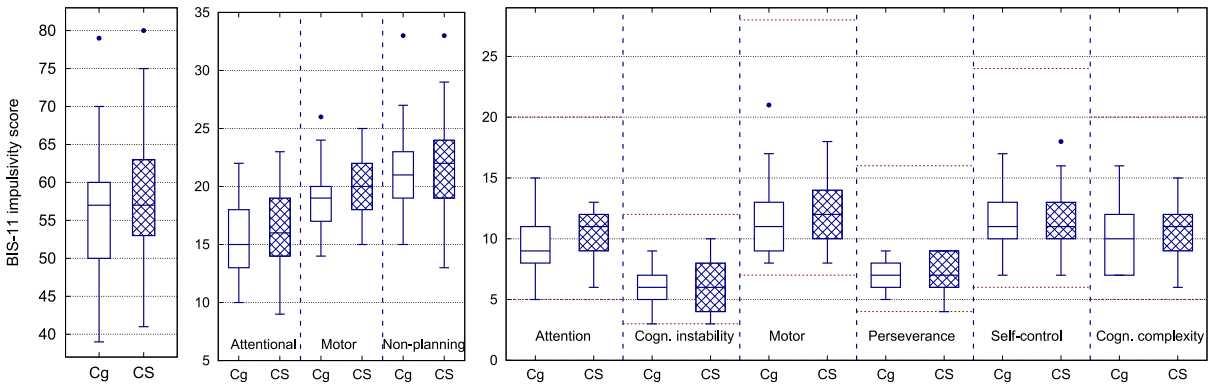
3.4. Demographic information

Participants of the experiment made two non-overlapping groups. The first participant group, a control group, comprised people who did not associate themselves with cybersecurity as a direct work focus area. The second participant group, a target group, consisted of people who identified themselves as cybersecurity specialists. We recruited 25 control individuals and 23 cybersecurity specialists in the model building and the PoC pilot. Informed written consent was obtained from each individual. The study participants represented the age group of 20–45 years, men and women from Lithuania.

The demographic information was collected using a questionnaire presented in Appendix A. Table 1 provides aggregated demographic information that falls within the scope of this paper. The participant was assigned to the target group when the answer to question no. 7 (*Are you a CS specialist?*) of the questionnaire was *Yes*. Also, the participant had to self-assign to the group when filling out participation documents as required according to the protocol defined in the research permission. The control group was more gender-balanced than the target group of CS specialists. Most of the CS specialists were associated with the IT field. Moreover, the control group had higher level degrees on average than the specialist group. For example, seven participants in the control group held a PhD degree, and eleven had a university-level master's degree. The specialist group mainly had college or university bachelor level education, with only ten having (in-)completed master's education. The control group was slightly older than the specialist group, with a median age of 34 and 30, respectively.

3.5. Data analysis

Boxplot visualisations were used to illustrate and identify the statistical distribution of the scores supported by the BIS-11 questionnaire. They provided a high-level information about the participant groups, e.g., outliers, median values, and data variance. A heatmap was generated to determine significant differences in answers to individual BIS questions considering control and target groups. The boxplots and heatmap were prepared using the multi-platform command-line-based



(a) Impulsivity. (b) 2nd order scores. (c) 1st order scores.

Fig. 6. Results of the BIS-11 impulsivity score. Cg - control group, CS - cybersecurity specialist group. The dots represent statistically defined outliers.

graphing utility Gnuplot version 5.4. Scatter plots with 2d density estimations with default settings were prepared using R software in RStudio release 2023.06.0+421.

For the genetic association analysis, we used Fisher's exact test as a first option in that kind of studies ($\alpha = 0.05$). It is more direct calculation than the alternative χ^2 method. Variants were tested for Hardy–Weinberg equilibrium ($p > 0.05$). For the variant effect size estimation odds ratio (OR) was calculated according to Altman [74].

We defined the following null hypotheses regarding the scores (10 in total) supported the BIS-inventory:

H_0^A *There is no difference between the BIS-score A for the cybersecurity group compared to the control group, where A is one of 10 BIS-supported scores, i.e., the groups are equivalent.*

The null hypothesis would be rejected if the p-value is less than 0.05. The Mann–Whitney U test was executed for two independent groups using *wilcox.test* that conducts the Mann–Whitney U test by default in R software.

4. Results

Firstly, BIS scores are analysed to answer RQ1 and identify differences (if any) between the specialist and control group regarding impulsivity-related factors that impact self-regulation. Fig. 6 presents the BIS scores of the data sample as a statistical distribution where dots represent outliers. Note that subfigures have different scales. The total impulsivity score is calculated using all 30 items. Therefore, the theoretical range of the score is $[30 \dots 120]$. All BIS-11 questions have scores of four possible values of the Likert scale, $S = [1 \dots 4]$. The 2nd order scores include non-overlapping subsets of questions. *Attentional* consists of eight questions, and the other two scores, *Motor* and *Non-planning*, include 11 questions each. Each 1st order score, composed of 3–7 questions, is a part of a particular 2nd order score. Limits of each 1st order score are visible in the figure (see Fig. 6(c)).

The primary BIS-score value 52–71 represents regular impulsivity, and most of the participants fall into this impulsivity category. The higher score indicates higher impulsivity. Therefore, both groups represent a population with regular impulsivity, with few participants who are very impulsive or not impulsive. The median ($\tilde{m}$) of the impulsivity score of both sample groups is the same (see Fig. 6(a)). The interval of the specialist group's second and third quartiles is shifted towards impulsivity. Nevertheless, the specialist group has a longer third quartile than the second one. At the same time, the control group has an inverted case. Moreover, the whole interval of results of the specialist group starts and ends later than in the control group. The control group results (2nd quartile values less than 52) show that the group contains more participants with high self-regulation (or they avoided answering honestly, as indicated in the inventory descriptions). The results of the Mann–Whitney U test show that groups are identical in terms of the impulsivity score ($W = 258.5, p = 0.5558$, $\tilde{m} = 57$ in both groups, and $IQR^{Cg} = 10$ and $IQR^{CS} = 9$; IQR is the Interquartile Range).

Within the second-order scores (see Fig. 6(b)), all medians within a group of cybersecurity specialists have higher values by two points compared to the control group, showing a higher impulsivity trend. The whole interval of results is also shifted up, but for *Attentional* (poor attention and cognitive instability) and *Non-planning* (poor self-control and cognitive complexity) impulsiveness, the interval is longer than within the control group. *Motor* impulsiveness median shows similar size quartiles two and three (higher impulsivity than in a control group), meaning more intensive motor activity and lower perseverance. But participants of both groups fall into good perseverance level. The results of the Mann–Whitney U test show that groups are identical in terms of the 2nd order impulsivity scores—*Attentional* ($W = 242.5, p = 0.3504$, $\tilde{m}^{Cg} = 15$, $\tilde{m}^{CS} = 16$, $IQR^{Cg} = 5$, and $IQR^{CS} = 4$), *Motor* ($W = 233, p = 0.2612$, $\tilde{m}^{Cg} = 19$, $\tilde{m}^{CS} = 20$, $IQR^{Cg} = 3$, and $IQR^{CS} = 3.5$), and *Non-planning* ($W = 271.5, p = 0.7479$, $\tilde{m}^{Cg} = 21$, $\tilde{m}^{CS} = 22$, $IQR^{Cg} = 4$, and $IQR^{CS} = 4.5$) have $p > 0.05$ with Motor characteristic most closer to $p = 0.05$ among all three score types.

The results of the first-order factors indicate similar trends for *Self-control* in both groups (good self-control). Higher *Perseverance* (related to a stable lifestyle and persistence) and *Attention* (related to focusing on current tasks) scores are more common in the specialist group than in the control group. Furthermore, the *Cognitive instability* (intruding thoughts) and *Cognitive complexity* (enjoying mental challenges) values of half of the participants fall into the longer and shorter intervals, respectively, in the specialist group than in the control group. *Motor impulsiveness* scores are shifted up in the specialist group even though the lowest quartile starts at the same place. It is important to notice that the six first-order and three second-order characteristics are not comparable by value as they have different counts of items, i.e., they have different minimum and maximum values. For example, the *Perseverance* score considers four items, *Cognitive instability* is calculated using three items, the *Self-control* score is aggregated using six items, and the *Non-planning* calculation requires 11 items. In Fig. 6(c), horizontal dotted lines identify the characteristic score limits. The results of the Mann–Whitney U test show that groups are not different in terms of the 1st order impulsivity scores— *Attention* ($W = 223.5, p = 0.1857$, $\tilde{m}^{Cg} = 9$, $\tilde{m}^{CS} = 11$, $IQR^{Cg} = 3$, and $IQR^{CS} = 2$), *Cognitive instability* ($W = 281.5, p = 0.9083$, $\tilde{m}^{Cg} = 6$, $\tilde{m}^{CS} = 6$, $IQR^{Cg} = 2$, and $IQR^{CS} = 3$), *Motor* ($W = 245, p = 0.3827$, $\tilde{m}^{Cg} = 11$, $\tilde{m}^{CS} = 12$, $IQR^{Cg} = 4$, and $IQR^{CS} = 4$), *Perseverance* ($W = 226.5, p = 0.1979$, $\tilde{m}^{Cg} = 7$, $\tilde{m}^{CS} = 7$, $IQR^{Cg} = 2$, and $IQR^{CS} = 2.5$), *Self-control* ($W = 312.5, p = 0.6099$, $\tilde{m}^{Cg} = 11$, $\tilde{m}^{CS} = 11$, $IQR^{Cg} = 3$, and $IQR^{CS} = 2.5$), and *Cognitive complexity* ($W = 228.5, p = 0.2219$, $\tilde{m}^{Cg} = 10$, $\tilde{m}^{CS} = 11$, $IQR^{Cg} = 5$, and $IQR^{CS} = 2.5$).

Individual answers to BIS questions (see questions in Appendix B) reveal individual self-reported attitudes and allow to answer RQ2.

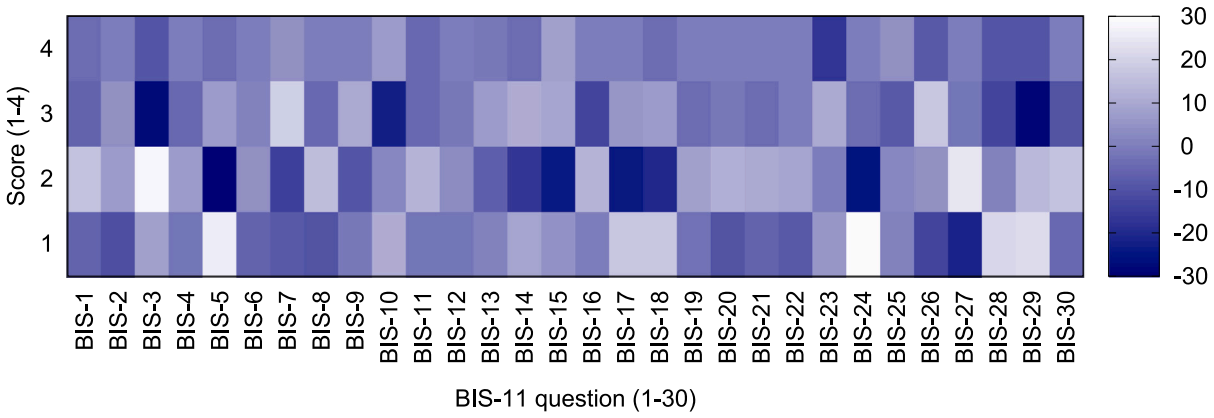
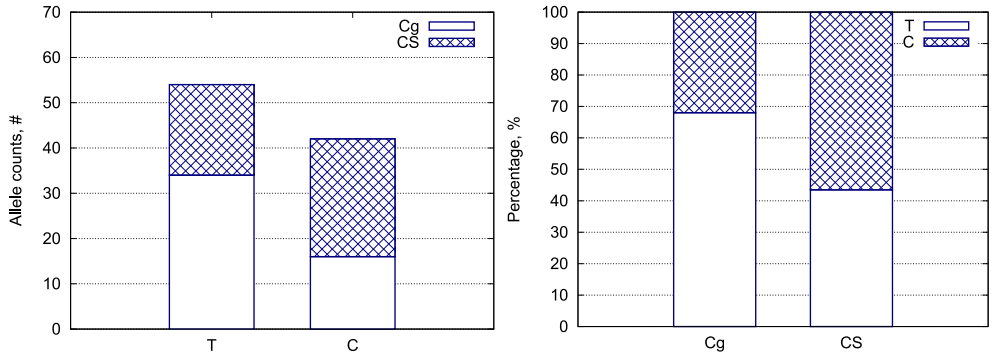


Fig. 7. A heatmap of individual BIS-11 questions (difference in control and specialist groups). (For interpretation of the references to colour in this figure legend, the reader is referred to the web version of this article.)



(a) Allele counts. (b) Allele distribution.

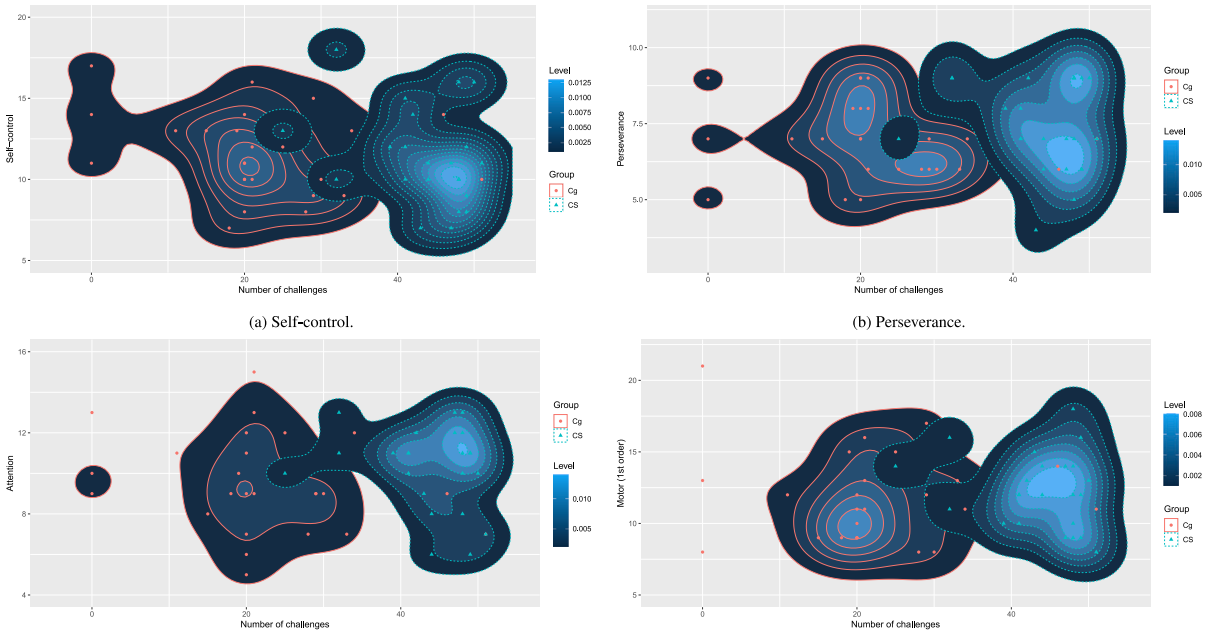
Fig. 8. Distribution of genetic variant rs6872863 alleles among study groups. Cg - control group, CS - cybersecurity specialist group; T - wild type allele of DNA sequence at position 60792321 on chromosome five, C - variant allele.

Fig. 7 identifies differences in answers to individual questions of two participant groups. The y-axis represents the value of the response. BIS-11 questions have scores of four possible values of the BIS Likert scale, $S = [1 \dots 4]$. The x-axis represents questions, $|BIS| = 30$. A heatmap was generated to determine significant differences in answers to individual questions considering control and target groups. The heatmap matrix H is calculated using normalised distributions of scores per answer, $H(i,j) = H^{Cg}(i,j) - H^{CS}(i,j)$, where $i \in S, j \in BIS$, and $\forall G \in \{Cg, CS\}, b \in BIS : \sum_{i \in S} H^{G}(i,b) = 100$. When the part of the results with the particular score is similar in both groups, then the difference is close to 0, and the colour in the heatmap is medium blue. When the part of the results in the control group Cg is more significant than in the specialist group CS, then the difference is a positive value. The greater the difference, the lighter the colour of the cell. Otherwise, the colour goes darker. For example, BIS-5 is a statement: "I make up my mind quickly", and the answer "Always" is worth 4 points. In the control group, 68% answered "Occasionally" (20%—"Often"), and among specialists, the results were 39% and 47%, respectively. Thus, the difference is 29% (almost a white cell at BIS-3 in the figure) and −27% (dark cell). Question 29 ("I like puzzles") is inverted, and the answer "Rarely/Never" is worth 4 points. Thus, cybersecurity specialists are not fond of puzzles but make decisions relatively fast when needed.

The genetic component was implemented and executed to support the proposed model. The genetic association was found when the counts of rs6872863 alleles among two groups (controls and cybersecurity specialists) were compared ($p = 0.02$). The alternative allele (C) effect size was calculated with 95% confidence interval (OR = 2.76, 95% CI: 1.20 to 6.35). According to published guidelines on interpreting odds ratio, an OR value 2.76 represents a small effect size [75] (Small: $1.68 \leq$ OR < 3.47). This suggests a minor association between the alternative allele (C) and the cybersecurity specialists group compared to controls.

Fig. 8(a) shows the distribution of the genetic variant alleles. A wild-type allele is more common in a control group than in a specialist group.

Phase III involved the CTF activity, having several categories of challenges, from cyber hygiene to tasks requiring expert knowledge. Some next questions became available only after the participant answered particular questions correctly. All challenges were available for both participant groups. The cyber hygiene category included 20 challenges. The specialists tried all of them, and within a control group, three participants did not solve any challenges. Some control group participants did not complete the cyber hygiene challenges but tried some more complex tasks dedicated to ICT skills. The maximum number of solved challenges was 51 (one participant per group). Fig. 9 provides some insights into the four characteristics, self-control, perseverance, attention, and motor impulsivity, taking into account the number of solved challenges to answer research question RQ3. Scatter plots with 2d density estimations with default settings were prepared using R software. The figure presents density charts where the x-axis presents a number of solved challenges, and the y-axis presents the first-order score of the characteristic from the BIS-11 inventory. As mentioned at the beginning of the section, the y-axis of different characteristics has different scales due to a different number of considered questions. The subfigures distinguish the data of the specialist and control groups. The control group mostly solved challenges from the cyber hygiene category, so within a group, the scores concentrated at a value of 20 on the x-axis. Thus, all subfigures have a control group data identifiable on the left. Fig. 9 illustrates data clustering based on kernel-density



(a) Self-control.

(b) Perseverance.

(c) Attention.

(d) Motor impulsivity.

Fig. 9. A density chart for a number of solved challenges with respect to four selected characteristics.

estimation. The diagram shows whether the cohorts are distinct and whether the participants formed several clusters solving challenges.

The analysis of statistical distributions of the first-order scores (see Fig. 6(c)) showed no significant difference for the *Self-control* characteristic. Fig. 9(a) illustrates how the BIS score impacts the number of solved challenges, and the control group has an apparent concentration at a score of 10, plus the control group results are more widespread and with lower density at the same peak. Regarding *Perseverance* property (see Fig. 9(b)), both groups have two clusters, and the same number of solved challenges covers two groups of perseverance values in the specialist group. In the control group, clusters have different BIS scores. Fig. 9(c) illustrates results related to the *Attention* characteristic. The control groups' results do not have a clear centre, with data points scattered along both axes. At the same time, the data concentration is visible in the specialist group around BIS value 11 with an extended interval for the number of solved challenges. *Motor impulsiveness* (the first-order score) trends show higher motor impulsiveness in the statistical distribution (see Figs. 6(c)), and 9(d) complements the results. The control group's results show higher and more concentrated impulsivity even with some outlier trends ("islands" overlapping with a control group's results).

To summarise the results, we should note that the results above demonstrate testing of the BIS-11 features as a model case. We aim to test and develop a full pathway for future personalised risk assessment and testing approaches integrating behavioural and health questionnaires in the cybersecurity subject area.

5. Discussion

5.1. Theoretical implications

The current work presents, first to our knowledge, an interdisciplinary model with the experimental PoC, designed to advance the cybersecurity workforce by providing multifaceted triangulations on behaviour-related features essential for cybersecurity specialists. We hypothesise that there should be some features, e.g. the level of impulsivity and self-regulation/self-control, that are crucial factors in cybersecurity specialists' everyday work and could be the object of advancements considering other means of cross-validation.

From the BIS-11 inventory, we found that the overall impulsivity rate was higher in the cybersecurity specialist group when compared to controls (see Fig. 6). First-order scores such as attention, perseverance, motor impulsiveness, and cognitive complexity show differences between groups.

One way to answer research question RQ1 (about the typical self-regulation-related parameters of cybersecurity specialists compared to the general population) is to analyse genetic variation entities underlying some behavioural feature manifestations. Only to demonstrate how it could work, we took only one of the hundreds of possibly implicated genetic variants (variant ID number rs6872863). We found a statistically significant difference in the frequency of the variant forms (alleles) between the cybersecurity specialists and the control group. The "T" allele, the reference one, was more frequent in the control group, while the "C" allele, the alternative one, was more frequent in the cybersecurity specialist group. Following the genome-wide association studies (GWAS) central database, the rs6872863 was also found to be associated ($p \leq 0.05$) with some other phenotypes, such as systolic blood pressure, amyotrophic lateral sclerosis, and blood glucose level. There is evidence that the *ELOVL7* gene might be involved in a variety of biological pathways and cellular processes, e.g. in the androgen pathway and prostate carcinogenesis [76], milk production in mammary cells [77], and inflammation reaction [78]. Genetic variants that are in strong linkage disequilibrium with the *ELOVL7* gene variant rs6872863 were also associated with different traits, such as educational attainment, mathematical ability [79], household income [80], and brain morphology [81,82]. Multiple involvement of a variant and a gene is not uncommon for multi-factorial and complex traits but makes it difficult to interpret and is set for future investigations.

RQ2 was designed to analyse self-reported attitudes to everyday activities and behaviour using the BIS-11 inventory to gain insight into attitude trends in the cybersecurity workforce community. There were distinct differences in answers to some questions in both participant groups. As presented in Section 4, cybersecurity specialists make faster decisions than the control group. Thus, their self-control is vital during crises. Current research and educational strategies involve gamification details, e.g. puzzles are provided in training environments, assuming cybersecurity specialists enter the field because they like solving challenges. However, our preliminary results identified that

the specialists are not-liking puzzles. This self-reported result means that trainers should re-consider some training scenarios and provide options for those not interested in solving puzzles. This initial research cannot give an unambiguous answer to RQ2 yet. The research used an approved translation of the BIS-11 questionnaire. The localised translation of the concept "puzzle" represented a too-narrow meaning of challenges, requiring further investigations. However, the analysis of the BIS-11 inventory shows its potential for further research to provide educational and training recommendations, even challenging the existing research results (or complementing them) on education and cybersecurity exercises.

To answer RQ3, we have shown similarities and differences regarding impulsive behaviour (self-control, self-regulation and others) between target and control groups through different angles. It is important to emphasise that the environment influences behavioural patterns, and solving digital challenges might reflect the experience. Nevertheless, none of those may impact genetics. Our genetic findings support results found in the BIS-11 inventory, allowing us to triangulate answers in case of deliberate avoidance of honest answers. The existing heritability of self-control implies that distinct genetic profiles between individuals may partially explain personal differences in self-control behaviour (self-reported or demonstrated during professional activities). Thus, despite operating in an identical environment, a person who is genetically pre-disposed for lower self-control may have problems regulating their thoughts, behaviour and impulses, whereas a person who has a genetic propensity to be more self-controlled may not even notice the challenges of self-control [13]. These findings suggest that the environment, e.g. peers, decision-makers should take into account such inborn individual differences in personal self-control capacities [83].

5.2. Implications for practice

5.2.1. Limitations

Our study has external and internal limitations, and we have to identify those to build the basis for further research and practical implementations. Firstly, the sample size of the experimental part ($n = 48$) is modest. Still, for the sake of demonstration of the principle, it is sufficient. Secondly, we could not escape biases in the questionnaire. The research team believes that the research participants have higher perseverance and cognitive complexity characteristics already because they volunteered to participate in a procedure that involved multiple phases (arriving at the hospital premises, reading and filling document (consent), giving a blood sample, filling digital questionnaires, and finally solving ICT-related tasks).

As an internal limitation we acknowledge that genetic association analysis was performed with only one variant when analysis of complex behaviours should include much more. Yet again, the chosen approach was simple but illustrative enough to demonstrate the idea of the suggested concept. Genetic analysis could go further by including hundreds of variants, and this is planned for future research.

Finally, the triangulation did not include other data we collected such as decision-making in solving tasks, jumping among challenges, stopping solving tasks, reconnecting from home, and even brute forcing the tasks to get the correct answer. Even though the genetic component is the most complex to implement, it can be applied under particular circumstances to develop individual resilience and build necessary skills, e.g., in critical infrastructure and military operations.

5.2.2. Model evaluation and practical implementation

Advances in theory and research on self-regulation and decision-making processes have yielded important insights into how cognitive, emotional, and social processes shape risk perceptions and risk-related decisions. Cameron et al. [84] examined how self-regulation theory can be applied to inform our understanding of decision-making processes. Our proposed model allows us to gather self-reported data relating to behaviour traits and triangulate it with professional activities and genetic association results. Then, the result reveals the whole picture of individual risks. The model complements the existing research that emphasises the importance of considering the soft part of the person, avoiding the dedicated focus on technical skills. In this work, we demonstrate PoC, focusing on one characteristic. However, any characteristic can provide the information to consider when building the cyber workforce.

Personality traits are related to insider threats; thus, possible mitigations include training, increasing awareness of individual biases, or emotion- and logic-based influencers [85]. Maasberg et al. [86] have found that psychopathy of the dark triad strongly correlates to intentional malicious behaviour. They emphasise that managers should be aware of insiders that have dark triad traits to apply early mitigation techniques, e.g. psychopathy is characterised by high impulsiveness, leading to impulsive behaviour. Papatsaroucha et al. [87] conclude their research by saying that training techniques should include more methods to address the traits of each individual. Another research outlines a correlation between personal characteristics, such as impulsivity, risk-taking, and a disregard for future consequences of actions, and non-compliance with cyber and network security policies [88].

In addition to being informed or self-aware of some potential/ hidden/ unknown/ undiscovered behavioural traits, there is the possibility of intervening or even overcoming some actions or behaviours. An extensive meta-analysis of 49 randomised clinical trials involving 50 self-regulation interventions discovered that these interventions yielded positive results for children and adolescents [83]. Besides psychological methods [88] encouraging behaviours that advance security, cognitive training methods, e.g., cognitive control, help reduce security-threatening behaviours such as impulsivity and risk-taking [89]. With its proof of principle, our model makes a reasonable example of practical implementation for cybersecurity specialists at work. As Harden and Koellinger [90] put it: "ignoring the relevance of genes would mean ignoring an important part of reality, which could lead to erroneous and misleading conclusions about environmental or behavioural effects".

5.2.3. Ethics, law, social and political aspects

Ethics plays a crucial role in ensuring the responsible application of behaviour genetics research, promoting respect for individuals' autonomy, privacy, and well-being. Around behaviour genetic application, there were always numerous ethical concerns. First of all, genetic determinism. The misconception of genetic factors' influence on behavioural traits can lead to stigmatisation or discrimination against individuals with specific genetic characteristics. Thus, genetic results should be communicated with care and accuracy, ensuring equity and fairness. Medicalising behaviour traits could lead to discrimination, mistreatment, and abuse of information in employment processes or personal social activities, e.g., signing insurance contracts. That is why it is crucial to guarantee privacy and confidentiality.

In best case scenarios, introducing genetic factors into the application process could serve a positive goal by helping individuals receive better training or open wider occupational opportunities. Even though genetic screening related to the workplace suggests new research and application directions, it must be conducted according to law and medical and ethical standards, including valid scientific practices [91]. The benefits should be measured over the potential risks. Being mindful of the potential psychological impact of genetic information, we have to apply behaviour genetic research responsibly in the development of policies and regulations, avoiding discriminatory practices or unjust societal interventions. Consent and the opportunity for screened persons to discuss the results with a professional are essential components in understanding screening limitations and avoiding uncertainties in interpretation.

Some measures could be taken to mitigate the consequences related to genetic testing. The first and most crucial part is informed consent before undergoing any genetic testing. It provides clear and comprehensive information about the potential risks, benefits, and

implications of the testing results. An individual has to understand who will have access to their genetic information and how it will be used [92]. Transparency and public awareness can also play a valuable role. By increasing public awareness of genetic testing, its benefits, and potential risks, we can empower individuals to make informed choices. Transparency from genetic testing companies about their data handling practices and potential risks can also build trust with consumers [93]. Solid policies and regulations addressing privacy and confidentiality protection include safeguarding data from unauthorised access and ensuring that genetic information is not disclosed without individual consent [94]. Implementing robust cybersecurity measures and regularly updating privacy policies can help mitigate risks. Laws such as the Working Document on Genetic Data in the EU [95] as well as the Genetic Information Nondiscrimination Act (GINA) [96] in the United States prohibit discrimination based on genetic information in health insurance and employment. The development and enforcement of ethical guidelines for genetic testing is essential. Regulatory oversight (by established regulatory bodies) must be implemented to ensure compliance with ethical standards and legal requirements regarding genetic testing practices. These bodies can monitor, conduct audits, and address any breaches of privacy or confidentiality [94,97]. Professionals involved in genetic testing should receive training on the ethical, legal, and social implications of genetic information. This practice ensures that they can handle sensitive information responsibly and ethically [97].

6. Conclusions and future work

Our study aimed to model a multifaceted experimentation environment to investigate the essential factors for cybersecurity specialists and propose interdisciplinary insights to advance their work. Through the hypothetical model and study design, the PoC implementation demonstrated how this interdisciplinary model could work. The chosen BIS-11 inventory enabled the analysis of aggregated scores and individual attitudes to raise concerns and questions about the typical understanding of the cybersecurity specialist persona. The initial results of this study show that more profound behavioural research can contradict the latter. The analysis also demonstrated higher BIS scores, e.g., motor impulsivity, yet not statistically significantly different; thus, it supported the existing research that the digital environment requires motor impulsiveness to act and make decisions. However, further research is needed to identify and prove distinctive features and trait-related risks to make training recommendations sound. Genetic data was used to test behavioural trait-related genetic variants, providing additional insight into the cybersecurity management field. The study reviews related research and suggests that self-regulation and impulsivity play a significant role in decision-making and cybersecurity work, and addressing individual differences in self-control capacities could be crucial. We also emphasise the need for ethical considerations in the application of behaviour genetics in the workplace, ensuring proper consent and professional interpretation of results. Overall, this interdisciplinary approach shows promise in advancing the cybersecurity workforce through multifaceted recommendations based on essential behavioural features.

In the future, we plan to investigate and evaluate multiple parametric correlations, considering more entities participating in the experiment. As a possible future direction, we envision focusing on the cybersecurity competence level evaluation, designing the personalised risk assessment metrics, and finding parameters relating to health data in a complex environment to describe behavioural patterns in certain situations.

CRediT authorship contribution statement

Agnė Brilingaitė: Writing – review & editing, Writing – original draft, Visualization, Project administration, Methodology, Investigation, Formal analysis, Data curation. **Linas Bukauskas:** Writing – review & editing, Writing – original draft, Visualization, Validation, Software, Resources, Methodology, Investigation, Data curation, Conceptualization. **Ingrida Domarkienė:** Writing – review & editing, Writing – original draft, Resources, Investigation, Formal analysis, Data curation, Conceptualization. **Tautvydas Rančelis:** Writing – original draft, Validation, Resources, Methodology, Investigation, Formal analysis, Data curation, Conceptualization. **Laima Ambrozaitytė:** Writing – review & editing, Writing – original draft, Resources, Methodology, Investigation, Conceptualization. **Rūta Pirta:** Writing – review & editing, Writing – original draft, Validation. **Ricardo G. Lugo:** Writing – original draft, Validation, Methodology. **Benjamin J. Knox:** Writing – review & editing, Methodology.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgements

The "Advancing Human Performance in Cybersecurity", ADVANCES, benefits from nearly €1 million grant from Iceland, Liechtenstein and Norway through the EEA Grants. The aim of the project is to advance the performance of cybersecurity specialists by personalising the competence development path and risk assessment. The project contract with the Research Council of Lithuania (LMTLT) No is S-BMT-21-6 (LT08-2-LMT-K-01-051). The authors thank the ADVANCES team for providing feedback, raising questions during the discussions, and supporting the authors.

Appendix A. Questionnaire. general information

The questionnaire included several parts. This section covers *General information* that was used to gather demographic data about research participants. It was part of the application to get permission to perform the study (see permission number and granting authority in Section 3.3). Note that the education-related question follows the national education framework. The participants answered the following questions (in Lithuanian language):

1. Gender:
    (a) male
    (b) female
    (c) other
2. Age (years):
3. Height (cm):
4. Weight (kg):
5. Highest education level acquired:
    (a) incomplete secondary/ high school
    (b) secondary/high school
    (c) specific secondary/ high school degree or equivalent
    (d) incomplete college
    (e) college
    (f) incomplete bachelor's degree
    (g) bachelor's degree
    (h) incomplete master's degree
    (i) master's degree
    (j) incomplete doctoral studies

(k) doctoral degree
(l) other

6. Occupation:

(a) working
(b) studying
(c) other

7. Are you a CS specialist?

(a) Yes
(b) No

8. IT related Speciality/Profession:

(a) Yes
(b) No

9. Personal relationships:

(a) married
(b) single
(c) divorced
(d) widow
(e) living with the life partner
(f) no regular relationships
(g) in a relationship
(h) other

10. Do you have children? (If Yes—How many?)

(a) Yes
(b) No

The survey was presented to the participants in Lithuanian:

1. Lytis:

(a) Vyras
(b) Moteris
(c) Kita

2. Amžius (metais):
3. Ūgis (cm):
4. Svoris (kg)
5. Aukščiausias įgytas išsilavinimas:

(a) Nebaigtas vidurinis
(b) Vidurinis
(c) Specialusis vidurinis
(d) Nebaigtas aukštasis koleginis
(e) Aukštasis koleginis
(f) Nebaigtos universitetinės bakalauro studijos
(g) Universitetinis bakalauro laipsnis
(h) Nebaigtos universitetinės magistro studijos
(i) Universitetinis magistro laipsnis
(j) Nebaigtos doktorantūros studijos
(k) Mokslų daktaro laipsnis
(l) Kita

6. Darbo (veiklos) pobūdis:

(a) Dirbu
(b) Studijuoju
(c) Kita

7. Ar esate kibernetinio saugumo specialistas?

(a) Taip
(b) Ne

8. Specialybė/profesija susijusi su IT:

(a) Taip
(b) Ne

9. Šeimyninė padėtis:

(a) Vedęs/ištekėjusi
(b) Nevedęs/netekėjusi
(c) Išsiskyręs (-usi)
(d) Našlys (-ė)
(e) Turiu gyvenimo partnerę /partnerį
(f) Neturiu pastovių tarpasmeninių santykių
(g) Turiu pastovius tarpasmenininius santykius
(h) Kita

10. Ar turite vaikų? (Jei Taip—Kiek turite vaikų?):

(a) Taip
(b) Ne

Appendix B. Questionnaire. BIS-11 inventory

This section provides BIS-11 inventory [70,71] that was used in the study.

Filling out directions: People differ in the ways they act and think in different situations. This is a test to measure some of the ways in which you act and think. Read each statement and put an X on the appropriate circle on the right side of this page. Do not spend too much time on any statement. Answer quickly and honestly.

The answers are designed using a 4-point Likert scale (1—Rarely/Never, 2—Occasionally, 3—Often Almost, 4—Almost Always/Always).

1. I plan tasks carefully.
2. I do things without thinking.
3. I make-up my mind quickly.
4. I am happy-go-lucky.
5. I don't "pay attention".
6. I have "racing" thoughts.
7. I plan trips well ahead of time.
8. I am self controlled.
9. I concentrate easily.
10. I save regularly.
11. I "squirm" at plays or lectures.
12. I am a careful thinker.
13. I plan for job security.
14. I say things without thinking.
15. I like to think about complex problems.
16. I change jobs.
17. I act "on impulse".
18. I get easily bored when solving thought problems.
19. I act on the spur of the moment.
20. I am a steady thinker.
21. I change residences.
22. I buy things on impulse.
23. I can only think about one thing at a time.
24. I change hobbies.
25. I spend or charge more than I earn.
26. I often have extraneous thoughts when thinking.
27. I am more interested in the present than the future.
28. I am restless at the theater or lectures.
29. I like puzzles.
30. I am future oriented.

The questionnaire was provided in Lithuanian, and the Lithuanian version was prepared according to the previous validation research following the international recommendations [72].

1. Rūpestingai planuoju užduotis, kurias reikia atlikti
2. Elgiuosi neapgalvotai
3. Greitai apsisprendžiu
4. Esu nerūpestinga/-as
5. Sunkiai išlaikau dėmesį
6. Mano mintys labai greitai keičiasi
7. Keliones planuoju iš anksto
8. Gerai save kontroliuoju
9. Lengvai susikaupiu
10. Reguliariai atsidedu pinigų taupymui
11. Muistausi, jei reikia ilgiau išsėdėti
12. Viską rūpestingai apmąstau
13. Rūpinuos dėl savo darbo vietos užtikrintumo
14. Šneku neapgalvotai
15. Mėgstu galvoti apie sudėtingas problemas
16. Keičiu darbus
17. Elgiuosi impulsyviai
18. Man greitai pasidaro nuobodu sprendžiant protinių pastangų reikalaujančias užduotis
19. Imuosi veiksmų jų neapmąstęs
20. Nuolatos mąstau
21. Keičiu gyvenamąją vietą
22. Daiktus perku neapgalvotai
23. Vienu metu galiu galvoti tik apie vieną dalyką
24. Keičiu hobius, pomėgius
25. Išleidžiu daugiau nei uždirbu
26. Galvojant lenda pašalinės mintys
27. Mane labiau domina dabartis nei ateitis
28. Nenustygstu vietoje, jei reikia ilgiau išbūti ramiai
29. Mėgstu dėliones
30. Esu orientuotas į ateitį

Data availability

Data will be made available on request.

References

[1] European Union Agency for Cybersecurity, ENISA Foresight Cybersecurity Threats for 2030, ENISA Reports, 2023, URL https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030.

[2] (ISC)^2, Cybersecurity workforce study, 2022, https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf. (Accessed 18 July 2024).

[3] S. Furnell, The cybersecurity workforce and skills, Comput. Secur. 100 (2021) 102080, http://dx.doi.org/10.1016/j.cose.2020.102080.

[4] T. Maurer, A. Nelson, International Strategy to Better Protect the Financial System Against Cyber Threats, Tech. Rep., Carnegie Endowment for International Peace, 2020, p. 242, URL http://www.jstor.org/stable/resrep26915.10. (Accessed 19 July 2024).

[5] C. Radu, N. Smaili, Board gender diversity and corporate response to cyber risk: Evidence from cybersecurity related disclosure, J. Bus. Ethics 177 (2022) 351–374, http://dx.doi.org/10.1007/s10551-020-04717-9.

[6] K.-K. Moon, R.K. Christensen, Realizing the performance benefits of workforce diversity in the U.S. federal government: The moderating role of diversity climate, Public Pers. Manag. 49 (1) (2020) 141–165, http://dx.doi.org/10.1177/0091026019848458.

[7] J. Dawson, R. Thomson, The future cybersecurity workforce: Going beyond technical skills for successful cyber performance, Front. Psychol. 9 (2018) http://dx.doi.org/10.3389/fpsyg.2018.00744.

[8] W. Hofmann, B.J. Schmeichel, A.D. Baddeley, Executive functions and self-regulation, Trends in Cognitive Sciences 16 (3) (2012) 174–180, http://dx.doi.org/10.1016/j.tics.2012.01.006.

[9] B.J. Knox, R.G. Lugo, K. Helkala, S. Sütterlin, Slow education and cognitive agility: Improving military cyber cadet cognitive performance for better governance of cyberpower, Int. J. Cyber Warf. Terror. 9 (1) (2019) 48–66, http://dx.doi.org/10.4018/IJCWT.2019010104.

[10] C. Nobles, Establishing human factors programs to mitigate blind spots in cybersecurity, in: Midwest At AIS (MWAIS) 2019 Proceedings, vol. 22, AIS Electronic Library, 2019, pp. 1–7, URL https://aisel.aisnet.org/mwais2019/22/.

[11] O. Jøsok, R. Lugo, B.J. Knox, S. Sütterlin, K. Helkala, Self-regulation and cognitive agility in cyber operations, Front. Psychol. 10 (2019) http://dx.doi.org/10.3389/fpsyg.2019.00875.

[12] T.J.C. Polderman, B. Benyamin, C.A. De Leeuw, P.F. Sullivan, A. Van Bochoven, P.M. Visscher, D. Posthuma, Meta-analysis of the heritability of human traits based on fifty years of twin studies, Nature Genet. 47 (7) (2015) 702–709, http://dx.doi.org/10.1038/ng.3285.

[13] Y.E. Willems, N. Boesen, J. Li, C. Finkenauer, M. Bartels, The heritability of self-control: A meta-analysis, Neurosci. Biobehav. Rev. 100 (2019) 324–334, http://dx.doi.org/10.1016/j.neubiorev.2019.02.012.

[14] T.T. Morris, S. von Hinke, L. Pike, N.R. Ingram, G. Davey Smith, M.R. Munafò, N.M. Davies, Implications of the genomic revolution for education research and policy, Br. Educ. Res. J. 00 (2022) 1–21, http://dx.doi.org/10.1002/berj.3784.

[15] M.J. Taylor, Data protection, shared (genetic) data and genetic discrimination, Med. Law Int. 8 (1) (2006) 51–77, http://dx.doi.org/10.1177/096853320600800103.

[16] R. Petersen, D. Santos, M.C. Smith, K.A. Wetzel, G. Witte, Workforce Framework for Cybersecurity (NICE Framework), NIST Special Publication 800–181, National Institute of Standards and Technology, 2020, http://dx.doi.org/10.6028/NIST.SP.800-181r1.

[17] E.U.A. for Cybersecurity, European Cybersecurity Skills Framework (ECSF), ENISA Reports, 2022, URL https://www.enisa.europa.eu/publications/european-cybersecurity-skills-framework-role-profiles.

[18] Optiv Security Inc., The state of the CISO, 2019, https://www.optiv.com/sites/default/files/2019-09/Brand_CISO-ResearchStudy_Report_091719.pdf. (Accessed 19 July 2024).

[19] B. Cerin, Cyber security risk is a board-level issue, in: 2020 43rd International Convention on Information, Communication and Electronic Technology, MIPRO, 2020, pp. 384–388, http://dx.doi.org/10.23919/MIPRO48935.2020.9245151.

[20] A. Georgiadou, S. Mouzakitis, D. Askounis, Detecting insider threat via a cybersecurity culture framework, J. Comput. Inf. Syst. 62 (4) (2022) 706–716, http://dx.doi.org/10.1080/08874417.2021.1903367.

[21] Q.A. Aigbefo, Y. Blount, M. Marrone, The influence of hardiness and habit on security behaviour intention, Behav. Inf. Technol. 41 (6) (2022) 1151–1170, http://dx.doi.org/10.1080/0144929X.2020.1856928.

[22] M. Gratian, S. Bandi, M. Cukier, J. Dykstra, A. Ginther, Correlating human traits and cyber security behavior intentions, Comput. Secur. 73 (4) (2018) 345–358, http://dx.doi.org/10.1016/j.cose.2017.11.015.

[23] A.N. Joinson, M. Dixon, L. Coventry, P. Briggs, Development of a new 'human cyber-resilience scale', J. Cybersecur. 9 (1) (2023) tyad007, http://dx.doi.org/10.1093/cybsec/tyad007.

[24] J. Hajny, S. Ricci, E. Piesarskas, O. Levillain, L. Galletta, R. De Nicola, Framework, tools and good practices for cybersecurity curricula, IEEE Access 9 (2021) 94723–94747, http://dx.doi.org/10.1109/ACCESS.2021.3093952.

[25] J. Haney, W. Lutters, J. Jacobs, Cybersecurity advocates: Force multipliers in security behavior change, IEEE Secur. Priv. 19 (4) (2021) 54–59, http://dx.doi.org/10.1109/MSEC.2021.3077405.

[26] N. Robinson, Human factors security engineering: The future of cybersecurity teams, EDPACS 67 (5) (2023) 1–17, http://dx.doi.org/10.1080/07366981.2023.2211429.

[27] N.H. Chowdhury, M.T.P. Adam, G. Skinner, The impact of time pressure on cybersecurity behaviour: A systematic literature review, Behav. Inf. Technol. 38 (12) (2019) 1290–1308, http://dx.doi.org/10.1080/0144929X.2019.1583769.

[28] C.M. Graham, Y. Lu, Skills expectations in cybersecurity: Semantic network analysis of job advertisements, J. Comput. Inf. Syst. 63 (4) (2023) 937–949, http://dx.doi.org/10.1080/08874417.2022.2115954.

[29] K.H. Pherson, R.H. Pherson, Critical Thinking for Strategic Intelligence, CQ Press, 2020.

[30] B. Fund, 16 soft skills you need to succeed in cyber security, 2021, URL https://flatironschool.com/blog/soft-skills-cyber-security. (Accessed 2 April 2024).

[31] F. Scholl, Developing your portfolio of soft skills for cybersecurity, 2020, URL https://quonline.quinnipiac.edu/blog/developing-your-portfolio-of-soft-skills-for-cybersecurity.php/.

[32] M. Waqas, A. Hania, F. Yahya, I. Malik, Enhancing cybersecurity: The crucial role of self-regulation, information processing, and financial knowledge in combating phishing attacks, SAGE Open 13 (4) (2023) 21582440231217720, http://dx.doi.org/10.1177/21582440231217720.

[33] S. Sheng, M. Holbrook, P. Kumaraguru, L.F. Cranor, J. Downs, Who falls for phish? A demographic analysis of phishing susceptibility and effectiveness of interventions, in: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems, CHI '10, Association for Computing Machinery, 2010, pp. 373–382, http://dx.doi.org/10.1145/1753326.1753383.

[34] J. Steinke, B. Bolunmez, L. Fletcher, V. Wang, A.J. Tomassetti, K.M. Repchick, S.J. Zaccaro, R.S. Dalal, L.E. Tetrick, Improving cybersecurity incident response team effectiveness using teams-based research, IEEE Secur. Priv. 13 (4) (2015) 20–29, http://dx.doi.org/10.1109/MSP.2015.71.

[35] P. Ifinedo, Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors, J. Comput. Inf. Syst. 63 (2) (2023) 380–396, http://dx.doi.org/10.1080/08874417.2022.2065553.

[36] J.H. Flavell, Metacognition and cognitive monitoring: A new area of cognitive–developmental inquiry, Am. Psychol. 34 (10) (1979) 906, http://dx.doi.org/10.1037/0003-066X.34.10.906.
[37] J. Suss, P. Ward, Revealing perceptual–cognitive expertise in law enforcement: An iterative approach using verbal-report, temporal-occlusion, and option-generation methods, Cogn. Technol. Work 20 (2018) 585–596, http://dx.doi.org/10.1007/s10111-018-0493-z.
[38] M. Thangavelu, V. Krishnaswamy, M. Sharma, Impact of comprehensive information security awareness and cognitive characteristics on security incident management — An empirical study, Comput. Secur. 109 (2021) 102401, http://dx.doi.org/10.1016/j.cose.2021.102401.
[39] A. Bandura, Social foundations of thought and action, Prentice-Hall, Inc, Englewood Cliffs, NJ, 1986, p. 617.
[40] B.J. Zimmerman, Chapter 2 - attaining self-regulation: A social cognitive perspective, in: M. Boekaerts, P.R. Pintrich, M. Zeidner (Eds.), Handbook of Self-Regulation, Academic Press, San Diego, 2000, pp. 13–39, http://dx.doi.org/10.1016/B978-012109890-2/50031-7.
[41] C.S. Carver, M.F. Scheier, On the Self-Regulation of Behavior, Cambridge University Press, 2001.
[42] M. Gillebaart, The 'operational' definition of self-control, Front. Psychol. 9 (2018) 1231, http://dx.doi.org/10.3389/fpsyg.2018.01231.
[43] D.W. Murray, K. Rosanbalm, C. Christopoulos, A.L. Meyer, An applied contextual model for promoting self-regulation enactment across development: Implications for prevention, public health and future research, J. Prim. Prev. 40 (2019) 367–403, http://dx.doi.org/10.1007/s10935-019-00556-1.
[44] N.A. Fox, S.D. Calkins, The development of self-control of emotion: Intrinsic and extrinsic influences, Motiv. Emot. 27 (2003) 7–26, http://dx.doi.org/10.1023/A:1023622324898.
[45] K.P. Harden, K.L. Klump, Introduction to the special issue on gene-hormone interplay, Behav. Genet. 45 (2015) 263–267, http://dx.doi.org/10.1007/s10519-015-9717-7.
[46] K.E. Boyle, H.T. Monaco, M. Deforet, J. Yan, Z. Wang, K. Rhee, J.B. Xavier, Metabolism and the evolution of social behavior, Mol. Biol. Evol. 34 (9) (2017) 2367–2379, http://dx.doi.org/10.1093/molbev/msx174.
[47] R. Lauretta, M. Sansone, A. Sansone, F. Romanelli, M. Appetecchia, Gender in endocrine diseases: Role of sex gonadal hormones, Int. J. Endocrinol. 2018 (1) (2018) 4847376, http://dx.doi.org/10.1155/2018/4847376.
[48] C.S. Carter, Hormonal influences on human behavior, in: A. Schmitt, K. Atzwanger, K. Grammer, K. Schäfer (Eds.), New Aspects of Human Ethology, Springer US, Boston, MA, 1997, pp. 141–162, http://dx.doi.org/10.1007/978-0-585-34289-4_8.
[49] G.S. Hotamisligil, R.J. Davis, Cell signaling and stress responses, Cold Spring Harb. Perspect. Biol. 8 (10) (2016) a006072, http://dx.doi.org/10.1101/cshperspect.a006072.
[50] J.-H. Baik, Stress and the dopaminergic reward system, Exp. Mol. Med. 52 (12) (2020) 1879–1890, http://dx.doi.org/10.1038/s12276-020-00532-4.
[51] F. Chaouloff, Serotonin, stress and corticoids, J. Psychopharmacol. 14 (2) (2000) 139–151, http://dx.doi.org/10.1177/026988110001400203.
[52] G.B. Glavin, Stress and brain noradrenaline: A review, Neurosci. Biobehav. Rev. 9 (2) (1985) 233–243, http://dx.doi.org/10.1016/0149-7634(85)90048-X.
[53] D.J. Bridgett, N.M. Burt, E.S. Edwards, K. Deater-Deckard, Intergenerational transmission of self-regulation: A multidisciplinary review and integrative conceptual framework, Psychol. Bull. 141 (3) (2015) 602–654, http://dx.doi.org/10.1037/a0038662.
[54] A.J. Ellis, C.G. Beevers, J.G. Hixon, J.E. McGeary, Serotonin transporter promoter region (5-HTTLPR) polymorphism predicts resting respiratory sinus arrhythmia, Psychophysiology 48 (7) (2011) 923–926, http://dx.doi.org/10.1111/j.1469-8986.2010.01154.x.
[55] R.H. Anderberg, C. Hansson, M. Fenander, J.E. Richard, S.L. Dickson, H. Nissbrandt, F. Bergquist, K.P. Skibicka, The stomach-derived hormone ghrelin increases impulsive behavior, Neuropsychopharmacology 41 (5) (2016) 1199–1209, http://dx.doi.org/10.1038/npp.2015.297.
[56] L.A. D'Ambrosio, L.K.M. Donorfio, J.F. Coughlin, M. Mohyde, J. Meyer, Gender differences in self-regulation patterns and attitudes toward driving among older adults, J. Women Aging 20 (3–4) (2008) 265–282, http://dx.doi.org/10.1080/08952840801984758.
[57] N. Hosseini-Kamkar, J.B. Morton, Sex differences in self-regulation: An evolutionary perspective, Front. Neurosci. 8 (2014) 233, http://dx.doi.org/10.3389/fnins.2014.00233.
[58] L.D. van der Pol, M.G. Groeneveld, S.R. van Berkel, J.J. Endendijk, E.T. Hallers-Haalboom, J. Mesman, Fathers: The interplay between testosterone levels and self-control in relation to parenting quality, Horm. Behav. 112 (2019) 100–106, http://dx.doi.org/10.1016/j.yhbeh.2019.04.003.
[59] E. Mick, J. McGough, C.K. Deutsch, J.A. Frazier, D. Kennedy, R.J. Goldberg, Genome-wide association study of proneness to anger, PLoS One 9 (1) (2014) e87257, http://dx.doi.org/10.1371/journal.pone.0087257.
[60] J.C. Gray, J. MacKillop, J. Weafer, K.M. Hernandez, J. Gao, A.A. Palmer, H. de Wit, Genetic analysis of impulsive personality traits: Examination of a priori candidates and genome-wide variation, Psychiatry Res. 259 (2018) 398–404, http://dx.doi.org/10.1016/j.psychres.2017.10.047.
[61] S. Sanchez-Roige, P. Fontanillas, S.L. Elson, J.C. Gray, H. de Wit, J. MacKillop, A.A. Palmer, Genome-wide association studies of impulsive personality traits (BIS-11 and UPPS-P) and drug experimentation in up to 22,861 adult research participants identify loci in the CACNA1I and CADM2 genes, J. Neurosci. 39 (13) (2019) 2562–2572, http://dx.doi.org/10.1523/JNEUROSCI.2662-18.2019.
[62] R. Karlsson Linnér, T.T. Mallard, P.B. Barr, S. Sanchez-Roige, J.W. Madole, M.N. Driver, H.E. Poore, R. de Vlaming, A.D. Grotzinger, J.J. Tielbeek, et al., Multivariate analysis of 1.5 million people identifies genetic associations with traits related to self-regulation and addiction, Nature Neurosci. 24 (10) (2021) 1367–1376, http://dx.doi.org/10.1038/s41593-021-00908-3.
[63] H.G. Grasmick, C.R. Tittle, R.J. Bursik Jr., B.J. Arneklev, Testing the core empirical implications of Gottfredson and Hirschi's general theory of crime, J. Res. Crime Delinquency 30 (1) (1993) 5–29, http://dx.doi.org/10.1177/0022427893030001002.
[64] P. Ifinedo, Effects of security knowledge, self-control, and countermeasures on cybersecurity behaviors, J. Comput. Inf. Syst. 63 (2) (2023) 380–396, http://dx.doi.org/10.1080/08874417.2022.2065553.
[65] Y. Hong, S. Furnell, Understanding cybersecurity behavioral habits: Insights from situational support, J. Inform. Secur. Appl 57 (2021) 102710, http://dx.doi.org/10.1016/j.jisa.2020.102710.
[66] L. Hadlington, Human factors in cybersecurity; examining the link between internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours, Heliyon 3 (7) (2017) e00346, http://dx.doi.org/10.1016/j.heliyon.2017.e00346.
[67] M. Pattinson, M. Butavicius, K. Parsons, A. McCormac, D. Calic, Factors that influence information security behavior: An Australian web-based study, in: T. Tryfonas, I. Askoxylakis (Eds.), Human Aspects of Information Security, Privacy, and Trust, Springer International Publishing, Cham, 2015, pp. 231–241, http://dx.doi.org/10.1007/978-3-319-20376-8_21.
[68] L.M. Bishop, P.L. Morgan, P.M. Asquith, G. Raywood-Burke, A. Wedgbury, K. Jones, Examining human individual differences in cyber security and possible implications for human-machine interface design, in: A. Moallem (Ed.), HCI for Cybersecurity, Privacy and Trust, Springer International Publishing, Cham, 2020, pp. 51–66, http://dx.doi.org/10.1007/978-3-030-50309-3_4.
[69] Z. Aivazpour, V.S. Rao, Impulsivity and information disclosure: Implications for privacy paradox, in: Proc. of the 52nd Hawaii International Conference on System Sciences, 2019, pp. 4861–4874, URL http://hdl.handle.net/10125/59924.
[70] J.H. Patton, M.S. Stanford, E.S. Barratt, Factor structure of the barratt impulsiveness scale, J. Clin. Psychol. 51 (6) (1995) 768–774, http://dx.doi.org/10.1002/1097-4679(199511)51:6<768::aid-jclp2270510607>3.0.co;2-1.
[71] M.S. Stanford, C.W. Mathias, D.M. Dougherty, S.L. Lake, N.E. Anderson, J.H. Patton, Fifty years of the barratt impulsiveness scale: An update and review, Personal. Individ. Differ. 47 (5) (2009) 385–395, http://dx.doi.org/10.1016/j.paid.2009.04.008.
[72] J. Janavičiūtė, L. Šinkariova, Psychometric properties of the Lithuanian version of barratt impulsiveness scale-11 (BIS-11) in a nonclinical sample, Cogn. Brain Behav Interdiscip. J. 24 (2020) 123–138, http://dx.doi.org/10.24193/cbb.2020.24.07.
[73] N. Bouzidi, M. Hassine, H. Fodha, M. Ben Messaoud, F. Maatouk, H. Gamra, S. Ferchichi, Association of the methylene-tetrahydrofolate reductase gene rs1801133 C677T variant with serum homocysteine levels, and the severity of coronary artery disease, Sci. Rep. 10 (1) (2020) 10064, http://dx.doi.org/10.1038/s41598-020-66937-3.
[74] D.G. Altman, Practical Statistics for Medical Research, Chapman & Hall/CRC Texts in Statistical Science, London and New York, 1991.
[75] P.C. Henian Chen, S. Chen, How big is a big odds ratio? Interpreting the magnitudes of odds ratios in epidemiological studies, Comm. Statist. Simulation Comput. 39 (4) (2010) 860–864, http://dx.doi.org/10.1080/03610911003650383.
[76] W. Han, S. Gao, D. Barrett, M. Ahmed, D. Han, J.A. Macoska, H.H. He, C. Cai, Reactivation of androgen receptor-regulated lipid biosynthesis drives the progression of castration-resistant prostate cancer, Oncogene 37 (6) (2018) 710–721, http://dx.doi.org/10.1038/onc.2017.385.
[77] H. Shi, L. Wang, J. Luo, J. Liu, J.J. Loor, H. Liu, Fatty acid elongase 7 (ELOVL7) plays a role in the synthesis of long-chain unsaturated fatty acids in goat mammary epithelial cells, Animals 9 (6) (2019) 389, http://dx.doi.org/10.3390/ani9060389.
[78] Y. Inoue, T. Kamiya, H. Hara, Increased expression of ELOVL7 contributes to production of inflammatory cytokines in THP-1 cell-derived M1-like macrophages, J. Clin. Biochem. Nutr. 72 (3) (2023) 215, http://dx.doi.org/10.3164/jcbn.22-69.
[79] J.J. Lee, R. Wedow, A. Okbay, E. Kong, O. Maghzian, M. Zacher, T.A. Nguyen-Viet, P. Bowers, J. Sidorenko, R. Karlsson Linnér, et al., Gene discovery and polygenic prediction from a genome-wide association study of educational attainment in 1.1 million individuals, Nature Genet. 50 (8) (2018) 1112–1121, http://dx.doi.org/10.1038/s41588-018-0147-3.
[80] W.D. Hill, N.M. Davies, S.J. Ritchie, N.G. Skene, J. Bryois, S. Bell, E. Di Angelantonio, D.J. Roberts, S. Xueyi, G. Davies, et al., Genome-wide analysis identifies molecular systems and 149 genetic loci associated with income, Nature Commun. 10 (1) (2019) 5741, http://dx.doi.org/10.1038/s41467-019-13585-5.

[81] B. Zhao, T. Luo, T. Li, Y. Li, J. Zhang, Y. Shan, X. Wang, L. Yang, F. Zhou, Z. Zhu, et al., Genome-wide association analysis of 19,629 individuals identifies variants influencing regional brain volumes and refines their genetic co-architecture with cognitive and mental health traits, Nature Genet. 51 (11) (2019) 1637–1644, http://dx.doi.org/10.1038/s41588-019-0516-6.

[82] S. Sanchez-Roige, M.V. Jennings, H.H. Thorpe, J.E. Mallari, L.C. van der Werf, S.B. Bianchi, Y. Huang, C. Lee, T.T. Mallard, S.A. Barnes, et al., CADM2 is implicated in impulsive personality and numerous other traits by genome-and phenome-wide association studies in humans and mice, Transl. Psychiatry 13 (1) (2023) 167, http://dx.doi.org/10.1038/s41398-023-02453-y.

[83] A. Pandey, D. Hale, S. Das, A.-L. Goddings, S.-J. Blakemore, R.M. Viner, Effectiveness of universal self-regulation–based interventions in children and adolescents: A systematic review and meta-analysis, JAMA Pediatr. 172 (6) (2018) 566–575, http://dx.doi.org/10.1001/jamapediatrics.2018.0232.

[84] L.D. Cameron, B.B. Biesecker, E. Peters, J.M. Taber, W.M.P. Klein, Self-regulation principles underlying risk perception and decision making within the context of genomic testing, Soc. Personal. Psychol. Compass 11 (5) (2017) e12315, http://dx.doi.org/10.1111/spc3.12315.

[85] Carnegie Mellon University, Unintentional insider threats: A foundational study, 2013, http://dx.doi.org/10.1184/R1/6585575.v1, Report. URL https://kilthub.cmu.edu/articles/report/Unintentional_Insider_Threats_A_Foundational_Study/6585575.

[86] M. Maasberg, C. Van Slyke, S. Ellis, N. Beebe, The dark triad and insider threats in cyber security, Commun. ACM 63 (12) (2020) 64–80, http://dx.doi.org/10.1145/3408864.

[87] D. Papatsaroucha, Y. Nikoloudakis, I. Kefaloukos, E. Pallis, E.K. Markakis, A survey on human and personality vulnerability assessment in cyber-security: Challenges, approaches, and open issues, 2021, http://dx.doi.org/10.48550/arXiv.2106.09986, CoRR arXiv:2106.09986.

[88] A.A. Moustafa, A. Bello, A. Maurushat, The role of user behaviour in improving cyber security management, Front. Psychol. 12 (2021) 561011, http://dx.doi.org/10.3389/fpsyg.2021.561011.

[89] A.D. Peckham, S.L. Johnson, Cognitive control training for emotion-related impulsivity, Behav. Res. Ther. 105 (2018) 17–26, http://dx.doi.org/10.1016/j.brat.2018.03.009.

[90] K.P. Harden, P.D. Koellinger, Using genetics for social science, Nat. Hum. Behav. 4 (6) (2020) 567–576, http://dx.doi.org/10.1038/s41562-020-0862-5.

[91] P. Brandt-Rauf, J. Borak, D.C. Deubner, Genetic screening in the workplace, J. Occup. Environ. Med. 57 (3) (2015) e17–e18, http://dx.doi.org/10.1097/JOM.0000000000000417.

[92] Council of Europe, Convention for the protection of human rights and dignity of the human being with regard to the application of biology and medicine: Convention on human rights and biomedicine, 1997, European Treaty Series — No. 164, https://rm.coe.int/168007cf98, Oviedo.

[93] D. Stiles, P.S. Appelbaum, Cases in precision medicine: Concerns about privacy and discrimination after genomic sequencing, Ann. Intern. Med. 170 (10) (2019) 717–721, http://dx.doi.org/10.7326/M18-2666, PMID: 31060048.

[94] Institute of Medicine. Eds., L.B. Andrews, J.E. Fullarton, N.A. Holtzman, A.G. Motulsky, Assessing Genetic Risks: Implications for Health and Social Policy, National Academies Press, Washington, DC, 1994, http://dx.doi.org/10.17226/2057, URL https://nap.nationalacademies.org/catalog/2057/assessing-genetic-risks-implications-for-health-and-social-policy.

[95] European Commission, Article 29 Data Protection Working Party, Working document on genetic data, 2004, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2004/wp91_en.pdf. (Accessed 17 March 2004).

[96] U.S. Congress, Genetic information nondiscrimination act of 2008, 2008, https://www.congress.gov/bill/110th-congress/house-bill/493, Public Law 110-233, 122 Stat. 881.

[97] T. Ascencio-Carbajal, G. Saruwatari-Zavala, F. Navarro-Garcia, E. Frixione, Genetic/genomic testing: Defining the parameters for ethical, legal and social implications (ELSI), BMC Med. Ethics 22 (2021) 1–15, http://dx.doi.org/10.1186/s12910-021-00720-5.