TEAM WORK

Alessandro Annarelli, Silvia Bonomi, Silvia Colabianchi*, Fabio Nonino, Giulia Palombi, Alessandro Pompei, Leonardo Querzoni

Department of Computer, Control and Management Engineering Antonio Ruberti. Sapienza University of Rome.

**Corresponding author*

A MULTI-LAYER ATTACK MODEL INTEGRATING HUMAN FACTORS IN DELIVERING CYBERSECURITY

ABSTRACT

Questo studio propone un innovativo modello di attacco multilivello per la sicurezza informatica che integra livelli umani, di accesso e di rete. In particolare, si concentra sullo strato umano che è stato recentemente riconosciuto come una questione ancora aperta. Attingendo alla letteratura, vengono identificati i fattori umani (HF) che contribuiscono alle vulnerabilità informatiche e i comportamenti umani che possono portare a vulnerabilità. Infine, la ricerca discute le capacità umane che potrebbero essere sfruttate come fattori di mitigazione. Considerando gli HF da una duplice prospettiva, lo studio fornisce un approccio olistico che tiene conto sia degli elementi tecnici che di quelli umani nella gestione della sicurezza informatica.

This study proposes an innovative multi-layer attack model for cybersecurity that integrates human, access, and network layers. In particular, it focuses on the human layer which has been recently recognized as a still open issue. Drawing on literature, human factors (HFs) that contribute to cyber vulnerabilities and human behaviors that can lead to vulnerabilities are identified. Finally, the research discusses human capabilities that could be leveraged as mitigation factors. By considering the HFs from a twofold perspective, the study provides a holistic approach that accounts for both technical and human elements in cybersecurity management.

Introduction

Today's hyper-connected environment has led on one side to an appreciable increase in productivity, efficiency, and system integration and, on the other side, to an increased number of potential risks[1]. European policies are giving a strong impulse to the digitalization of enterprises to speed up their modernization, especially in the manufacturing domain[2]. This rapid digitalization has made organizations highly dependent on data and information belonging to

1. A. CORALLO, M. LAZOI, M. LEZZI, Cybersecurity in the context of industry 4.0: A structured classification of critical assets and business impacts, Comput Ind. 114 (2020).
2. DIGITAL, The DIGITAL Europe Programme – Work Programmes | Shaping Europe's digital future, (2021).

their integrated systems and opening new risk scenarios[3]; as a matter of fact, this dependency makes a cyber threat even more impactful in terms of continuity of business operations, theft of confidential information, and reputational harm. For these reasons, cybersecurity has become a top priority for organizations that are operating with increasingly dynamic and real-time optimized cyber socio-technical systems. Hazards are constantly changing, and threats and incidents become more sophisticated, forcing a continuous reconsideration of strategies to ensure operational continuity[4]. An attack model called Multi-Layer Attack Graph (MLAG) has been recently proposed[5] to capture the complexity and multiplicity of the cyber threats. The MLAG considers technical and non-technical vulnerabilities that can affect organizations by enlarging the perspective with respect to classical attack graph models and by considering different potential correlated dimensions where vulnerabilities may impact, i.e. at a human level, network access and credential level, and network level. Literature and daily practice suggest the need to further investigate the human role within the system, so this study focused on the identification of human factors and the vulnerabilities generated by individuals. Investigative activities conducted following numerous cyber incidents have traced at least part of their causes to human error or negligence, pointing to users as a weak link in the development of secure environments.

Therefore, countering cyber threats requires a focus on people and behaviors, not just technology. It is no longer enough to create a secure infrastructure; organizations must also address the human factors of cybersecurity by cultivating an informed and proactive workforc[6]. In this scenario, specific aspects of human and system errors are explored in cybersecurity discipline, but there is still a necessity to identify effective approaches which integrate human and technical aspects in a dynamic risk management framework focusing on threat and attack models, risk identification, and mitigation capabilities.

Hence, starting from a multi-layer attack graph reference model, this research is intended to be a first step towards defining a taxonomy of human factors, and classifying them with respect to human behaviors. Finally, the study identified human risk factors and capabilities that can mitigate the identified human vulnerabilities.

3. A. ANNARELLI, G. PALOMBI, Digitalization capabilities for sustainable cyber resilience: a conceptual framework, Sustainability (Switzerland). 13 (2021).

4. S. COLABIANCHI, F. COSTANTINO, G. DI GRAVIO, F. NONINO, R. PATRIARCA, Discussing resilience in the context of cyber physical systems, Comput Ind Eng. (2021) pp. 107534.

5. E.G. SPANAKIS, S. BONOMI, S. SFAKIANAKIS, G. SANTUCCI, S. LENTI, M. SORELLA, F.D. TANASACHE, A. PALLESCHI, C. CICCOTELLI, V. SAKKALIS, S. MAGALINI, Cyber-attacks and threats for healthcare - A multi-layer thread analysis, Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS. 2020-July (2020) pp. 5705–5708.

6. V. ZIMMERMANN, K. RENAUD, Moving from a 'human-as-problem'' to a 'human-as-solution'' cybersecurity mindset, International Journal of Human Computer Studies. 131 (2019) pp. 169–187.

Threat Modelling

Identifying threats is a challenging task for every organization since they may arise from many different perspectives. Concerning the cyber security domain, there are many different approaches and perspectives to elicit and identify threats related to the ICT infrastructure. Among the most relevant examples, the STRIDE[7] threat elicitation model is a software-centric approach, while the attack tree and attack graph models are asset-centric approaches. In this paper, we will focus on the attack graph model as it allows us to capture multiple points of view including the technical perspective, i.e. the actual environment under analysis and in particular the set of vulnerabilities affecting the environment, the asset perspective, i.e. the elements in the environment that are particularly relevant for the organization and the attacker perspective, i.e. the capabilities that an attacker should have to exploit the identified vulnerabilities and materialize the threat. In the literature, an attack graph (AG) is commonly considered a (graphical) representation of possible ways via which a potential attacker can intrude into the target network by exploiting a series of vulnerabilities on various network hosts and gaining certain privileges at each step. Many formalizations exist but, in general, a vertex of the attack graph represents privileges that an attacker may get over hosts (or devices) connected to the network and edges represent the vulnerabilities that may be exploited to gain additional privileges. For example, an attacker may exploit a software vulnerability to gain user level access on a web server and then, from this first foothold, exploit a second vulnerability in the operating system of the compromised machine to raise its privilege level to administrator, a favorable position to explore a larger attack surface on the host and the connected network. This scenario would be represented in the AG by two vertices representing user - and administrator- level privileges on the target host and an edge connecting them to represent the vulnerability. In the last 10 years, this model has been widely used to support different tasks like network hardening, risk analysis, and online detection, but it has currently a huge limitation: it can capture and represent only the ICT unit of the organization and to support the analysis of the level of exposure only from a technical perspective. Recently, an extension to this model, namely a Multi-Layer Attack Graph (MLAG) [5] model has been proposed to address this limitation and to consider also additional non-technical vulnerabilities that can affect the system enlarging the perspective and considering different layers. In the MLAG model, a threat is represented implicitly and strictly related to the notions of risk, asset, and vulnerability. Vulnerabilities and how they can

7. L.S. FERRO, A. MARRELLA, T. CATARCI, A Human Factor Approach to Threat Modeling, Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics). 12788 LNCS (2021) pp. 139–157.

be exploited in sequence to materialize a possible threat are at the heart of the model. The MLAG is based on the observation that an ICT network is not an isolated environment but interacts with many external factors, i.e., humans and processes, and such interactions may lead to the identification of additional threats enabled and driven by human factors and vulnerabilities. Thus, the MLAG includes multiple dimensions (shaped into layers) to capture all these relevant factors. This technique allows focusing on the vulnerabilities, on their exploits, and on the sequence in which possible exploits can be launched by the attacker. Any threat is inferred from the possible attack paths. The MLAG takes the same perspective as common AGs and models human vulnerabilities as a particular class of vulnerabilities that may provide privileges on the ICT system through the usage of access credentials. Thus, it introduces additional types of vertices and additional types of edges to represent and encode the fact that a human vulnerability, e.g., leaving the laptop unlocked while going out from the office, may provide the adversary with access to an ICT device (i.e., the connected laptop) from which the attacker has initial privileges on the network and can progress with an attack. The goal is to extend the notion of AGs and paths to multiple layers to provide a more complete view. The MLAG model supports the definition of attack paths through four different layers: human, access, business, and network. (Figure 1) shows an overview of these four layers to represent and analyze complex attack scenarios arising from the exploitation of both technical and non-technical vulnerabilities.

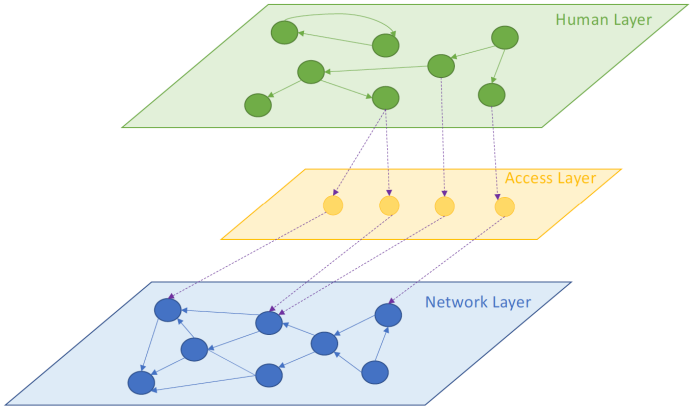

Fig. 1 - Multi-Layer Attack Graph (MLAG) Model

Thanks to its layer, MLAG allows to represent and to analyze an attack originating from an external attacker that exploits insecure human behaviors to get valid access to a device and then compromises the security of relevant assets reachable through the network. From a risk assessment perspective, all three layers (human, access, and network) can be the subject of hardening decisions

to various extents (i.e., mitigation actions can be both technical and non-technical and can be applied to any layer). When attacks lead to the failure of the organization's mission, they have a disruptive impact on business processes (business layer). Understanding the dependencies of assets (and their applications) is key to being able to correctly estimate the impact of attacks. While system vulnerabilities can be considered available information (i.e., they can be retrieved by automatic vulnerability scanners and analyzed using publicly available information e.g., those stored in NVD), identifying, classifying, and analyzing human vulnerabilities is still an open issue.

Human Factors & Vulnerabilities

The International Ergonomics Association defines human factors as the "scientific discipline concerned with the understanding of the interaction among humans and elements of the system"[8]. Human factors have been analyzed in various fields, especially the medical and aviation industries which have extensive work in this discipline[9]. Among the most famous classifications of human factors, in 2009 Dupont proposed "The Dirty Dozen"[10], a classification taken up by other fields such as healthcare and aviation[11,12] and useful also for cybersecurity[13]. Companies employing strong technology security policies frequently fail to address the human sources of vulnerability. Undoubtedly, the study of human factors is a research area neglected and underappreciated in cybersecurity[14]. Human engagement in information security is just too valuable for organizational leaders to continue ignoring the role of human behavior analysis in information security[15,16]. argued that empirical and theoretical research on human aspects of cybersecurity should be expanded based on the amount of human error-related occurrences to develop strategies to improve cybersecurity. Many classifications, ontologies, or just perspectives on what components of human character most affect cybersecurity have been offered throughout the

8. THE INTERNATIONAL ERGONOMICS ASSOCIATION, What Is Ergonomics (HFE)?, (2000).
9. S.A. SHAPPELL, D.A. WIEGMANN, A Human Error Approach to Aviation Accident Analysis: The Human Factors Analysis and Classification System, 2012.
10. G. DUPONT, Avoid the dirty dozen with safety nets, AIRBEATMAGAZINE. (2009).
11. D.N. POLLER, M. BONGIOVANNI, B. COCHAND-PRIOLLET, S.J. JOHNSON, M. PEREZ-MACHADO, A human factor event-based learning assessment tool for assessment of errors and diagnostic accuracy in histopathology and cytopathology, J Clin Pathol. 73 (2020) pp. 681–685.
12. A.G.A. SAMAD, M.K. JOHARI, S. OMAR, Preventing human error at an approved training organization using Dirty Dozen, International Journal of Engineering and Technology (UAE). 7 (2018) pp. 71–73.
13. G. DESOLDA, L.S. FERRO, A. MARRELLA, T. CATARCI, M.F. COSTABILE, Human Factors in Phishing Attacks: A Systematic Literature Review, ACM Comput Surv. 54 (2022).
14. A. OLTRAMARI, D. HENSHEL, M. CAINS, B. HOFFMAN, Towards a human factors ontology for cyber security, CEUR Workshop Proc. 1523 (2015) pp. 26–33.
15. SCIENCE OF SECURITY AND PRIVACY, Science of Security Annual Report 2015 | CPS-VO, 2015.
16. M. EVANS, L.A. MAGLARAS, Y. HE, H. JANICKE, Human behaviour as an aspect of cybersecurity assurance, Security and Communication Networks. 9 (2016) pp. 4667–4679.

years, with a focus on human factors and cybersecurity research. Characterization of human factors, including human behavior, is required above all to understand how the activities of users, defenders (IT workers), and attackers impact cybersecurity risk. However, a taxonomy that takes into account human factors, human behaviors, and the resulting cyber vulnerabilities that are being generated as far as the authors know is missing. In this first stage, the authors selected a human factor classification and through an exploration of the literature identified human behaviors linked. We chose the factors categorization proposed by Dupont[10] both because of its use in the cybersecurity field[13] and because sufficiently broad to include multiple subfactors useful in describing all critical issues. Dupont defines the twelve factors as the "Dirty Dozen"[10]. The name was chosen to reflect their negative connotation. The author emphasizes the necessity of understanding human elements that might lead to a mistake, regardless of scale, and suggest the "best way" for decreasing human error: (1) identify human factors, (2) implement human factors training and (3) create a work environment resistant to human mistakes. Dupont's list takes into account the following 12 factors:

- Lack of Communication;
- Complacency;
- Lack of Knowledge;
- Distraction;
- Lack of Teamwork;
- Fatigue;
- Lack of Resources;
- Pressure;
- Lack of assertiveness;
- Stress;
- Lack of awareness;
- Norms.

After selecting the classification, we used the human factors as keywords to identify determinants related to the human factors that generate cyber vulnerabilities in the relevant scientific literature. In addition, human factors and personality traits that characterize the user[17,18], generate risky cybersecurity behaviors that were also identified. The term risky behaviors refer to situations such as: not contacting IT support in case of an attack, sharing passwords with colleagues, deleting files due to distraction, or not reporting an incident[7,19]. Next, our study linked these identified factors with the vulnerabilities listed in[20] and in the updated version of the standar[21]. The document ISO/IEC 27005 provides guidelines for information security risk management. The document offers a list of vulnerabilities that apply to all types of businesses that want to manage risks that might undermine their information security. (Table 1) provides a detailed description of factors and associated behaviors and vulnerabilities.

Table 1 - Human Factors & Vulnerabilities

Human Factor	Definition	Vulnerabilities [20,21]
Lack of Communication	Communication is the act of sharing information between people using a shared system of symbols, signs, or behavior. When discussing cybersecurity, it means people communicating with one another in a working or online setting. This includes communication within work teams and with both internal and external stakeholders [22].	Insufficient clear desk and clear screen policy Email misuse Unsupervised work by outside or cleaning staff Insufficient security training
Complacency	The concept of complacency pertains to a sense of self-satisfaction or contentment with a current situation, where no further action is deemed necessary. Both in physical and cyber security, complacency refers to maintaining the current state during changing threats and requirements. In terms of attaining superior outcomes, complacency could be an indicator of overconfidence or lack of interest. Another possibility is that it could imply a degree of desensitization to online risks [23–25].	No 'log out' when leaving the workstation. Sharing credential Unprotected credential Non-compliance to policy on mobile computer usage Non-compliance with procedures for introducing software into operational systems. Email misuse Poor password management
Lack of Knowledge	Considering the diverse range of fields involved in organizational cybersecurity, it appears necessary to take a knowledge-based approach. To ensure the protection of intellectual property and maintain business continuity, cybersecurity management within an organization must prioritize knowledge management. As a result, it is suggested that taking a knowledge-based perspective on cybersecurity and its management could significantly affect the interactions between individuals, technology usage, and trust within the organization [26]	No 'log out' when leaving the workstation. Disposal or reuse of storage. media without proper erasure Sharing credential Unprotected credential Insufficient 'clear desk and clear screen' policy Non-compliance to policy on mobile computer usage Non-compliance with procedures for introducing software into operational systems. Email misuse Insufficient security training Poor password management
Distraction	Distractions hinder an individual's focus and can have cognitive consequences that extend beyond their assigned tasks. Distractions can interfere with our capacity to process information, and as a result, we tend to use heuristics to simplify information. Distractions in our cognitive processes not only impair our decision-making ability but also affect the extent to which we can be convinced by new information [27]	No 'log out' when leaving the workstation. Disposal or reuse of storage media without proper erasure. Non-compliance to policy on mobile computer usage Email misuse Poor password management

Lack of Teamwork	Teamwork involves collaborating with others to complete tasks. Many studies have emphasized the benefits of teamwork for the development of organizational skills. In the field of cybersecurity, effective cybersecurity teams can be created by bringing together domain-specific experts who work together and share their knowledge to achieve common objectives[28]	Insufficient 'clear desk and clear screen' policy Non-compliance with procedures for introducing software into operational systems Unsupervised work by outside or cleaning staff Insufficient security training
Fatigue	Cybersecurity fatigue is a unique form of professional disconnection within the field of cybersecurity. When an individual is exposed to cybersecurity instructions frequently, such as training or actions that align with cybersecurity procedures and practices, they can become exhausted and develop a reluctance towards the subject matter [25,29]	Sharing credential Unprotected credential Non-compliance to policy on mobile computer usage Non-compliance with procedures for introducing software into operational systems. Poor password management
Lack of Resources	Resources are the assets necessary to produce a product or deliver a service. In the context of cybersecurity, the business architecture of a company comprises a combination of people, processes, and technology [30]	Disposal or reuse of storage media without proper erasure. Non-compliance with procedures for introducing software into operational systems
Pressure	The term pressure refers to the mental strain resulting from the expectations to perform well in a particular situation. While some degree of pressure can positively impact performance, excessive pressure can lead to a decline in performance and choking.	Sharing credential Unprotected credential Email misuse
Stress	Stress is a state that triggers a psychophysiological reaction in an individual that disrupts their state of balance. In the realm of cybersecurity, stress can arise from multiple sources, including management initiatives, assignments of tasks and responsibilities, interpersonal clashes, and rules and procedures [31]	Disposal or reuse of storage media without proper erasure. Email misuse

17. M. GRATIAN, S. BANDI, M. CUKIER, J. DYKSTRA, A. GINTHER, Correlating human traits and cyber security behavior intentions, Comput Secur. 73 (2018) pp. 345–358.
18. S. UEBELACKER, S. QUIEL, The Social Engineering Personality Framework, Proceedings - 4th Workshop on Socio-Technical Aspects in Security and Trust, STAST 2014 - Co-Located with 27th IEEE Computer Security Foundations Symposium, CSF 2014 in the Vienna Summer of Logic 2014. (2014) pp. 24–30.
19. L. HADLINGTON, Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours, Heliyon. 3 (2017).
20. ISO/IEC 27005:2018, ISO - ISO/IEC 27005:2018 - Information technology — Security techniques — Information security risk management, (2018).
21. ISO/IEC 27005:2022, ISO - ISO/IEC 27005:2022 - Information security, cybersecurity and privacy protection — Guidance on managing information security risks, (2022).
22. L.E. POTTER, G. VICKERS, What skills do you need to work in cyber security? A look at the Australian market, SIGMIS-CPR 2015 - Proceedings of the 2015 ACM SIGMIS Conference on Computers and People Research. (2015) pp. 67–72.

Lack of assertiveness	Assertiveness refers to the ability to communicate one's opinions, viewpoints, ideas, or rights without invalidating those of others. This is an important skill in communication between employers and employees. A lack of proficiency in this area can negatively impact job performance. Assertiveness is a vital behavior that promotes positive relationships in the workplace and facilitates teamwork and decision-making, especially during critical situations [32]	Sharing credential Unprotected credential
Lack of awareness	The term awareness, in the context of cybersecurity, pertains to the process of acquiring knowledge that serves as a basis for altering individual and organizational attitudes and recognizing the significance of security and the adverse outcomes resulting from incidents. Research indicates that this goal can be accomplished through training and awareness-raising initiatives. In awareness-raising programs, the learner is the receiver of information, while in a training set, he or she takes on a more involved role [33,34]	No 'log out' when leaving the workstation. Disposal or reuse of storage media without proper erasure Sharing credential Unprotected credential Insufficient 'clear desk and clear screen' policy Non-compliance with procedures for introducing software into operational systems Email misuse Lack of security awareness Incorrect use of software and hardware Poor password management
Norms	The term norms refer to mutual expectations and shared beliefs concerning the appropriate behavior of actors belonging, for example, to an organization [35]	Disposal or reuse of storage media without proper erasure Sharing credential Unprotected credential Non-compliance to policy on mobile computer usage
		Non-compliance with procedures for introducing software into operational systems Unsupervised work by outside or cleaning staff Poor password management

23. K. PARSONS, A. MCCORMAC, M. BUTAVICIUS, M. PATTINSON, C. JERRAM, Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), Comput Secur. 42 (2014) pp. 165–176.
24. M. PATTINSON, M. BUTAVICIUS, K. PARSONS, A. MCCORMAC, D. CALIC, C. JERRAM, The information security awareness of bank employees, Proceedings of the 10th International Symposium on Human Aspects of Information Security and Assurance, HAISA 2016. (2016) pp. 189–198.
25. A. REEVES, P. DELFABBRO, D. CALIC, Encouraging Employee Engagement With Cybersecurity: How to Tackle Cyber Fatigue, Sage Open. 11 (2021).

These human factors, vulnerabilities, behaviors, and the relationships that emerged between them contribute to the characterization of individuals in a cybersecurity process. Furthermore, to enable a complete formulation of the human layer operating in the threat model shown above and for its application within organizations one must combine these considerations with specific assessments of the profile of the actors involved. In order to properly develop the model, it is essential to characterize each node of the human layer, using variables such as the individual's personality traits, behaviors, skills, and job duties. To do this, multiple formal questionnaires are available in the literature (e.g. Five Factor Model of personality[36,37], Human Aspects of Information Security Questionnaire[23], Organizational Information Security Culture Measure[38]) that have to be integrated and tailored with our findings on human factors in cybersecurity and with the context of their work activities (e.g., time in a current role that may contribute to their associated level of vulnerability for the environment). The questionnaire will return a cybersecurity profile for everyone (i.e., a set of characteristics that can describe and quantify their attitude toward cybersecurity in the context of their work activities). This value will serve in the formalization of the new human layer of the threat model.

26. M.P. SALLOS, A. GARCIA-PEREZ, D. BEDFORD, B. ORLANDO, Strategy and organisational cybersecurity: a knowledge-problem perspective, Journal of Intellectual Capital. 20 (2019) pp. 581–597.
27. L. MIARMI, K.G. DEBONO, The impact of distractions on heuristic processing: Internet advertisements and stereotype use, J Appl Soc Psychol. 37 (2007) pp. 539–548.
28. R.J. SIMONSON, J.R. KEEBLER, M. LESSMILLER, T. RICHARDS, J.C. LEE, Cybersecurity Teamwork: A Review of Current Practices and Suggested Improvements, Https://Doi.Org/10.1177/1071181320641101. 64 (2021) pp. 451–455.
29. S.M. KOMPASO, M.S. SRIDEVI, Employee Engagement: The Key to Improving Performance, International Journal of Business and Management. 5 (2010).
30. H. TAHERDOOST, Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview, Electronics (Switzerland). 11 (2022).
31. M. WEISS, Effects of work stress and social support on information systems managers*, MIS Quarterly. 7 (1983) pp. 29–43.
32. S.A. WOODS, J.A. SOFAT, Personality and engagement at work: The mediating role of psychological meaningfulness, J Appl Soc Psychol. 43 (2013) pp. 2203–2210.
33. CAMBRIDGE DICTIONARY, AWARENESS | English meaning - Cambridge Dictionary, (2022).
34. N.H. CHOWDHURY, M.T.P. ADAM, G. SKINNER, The impact of time pressure on cybersecurity behaviour: a systematic literature review, Behaviour and Information Technology. 38 (2019) pp. 1290–1308.
35. MICROSOFT, Microsoft Security Intelligence Report Volume 23 Supplement Malware at Microsoft 2, 2018.
36. R.R. MCCRAE, O.P. JOHN, An Introduction to the Five□Factor Model and Its Applications, J Pers. 60 (1992) pp. 175–215.
37. P.T. COSTA, R.R. MCCRAE, The Five-Factor Model, Five-Factor Theory, and Interpersonal Psychology, Handbook of Interpersonal Psychology: Theory, Research, Assessment, and Therapeutic Interventions. (2012) pp. 91–104.
38. K.M. PARSONS, E. YOUNG, M.A. BUTAVICIUS, A. MCCORMAC, M.R. PATTINSON, C. JERRAM, The Influence of Organizational Information Security Culture on Information Security Decision Making, Http://Dx.Doi.Org/10.1177/1555343415575152. 9 (2015) pp. 117–129.

Risk Mitigation Factors & Capabilities

According to what emerged from the academic literature and managerial context, nowadays human factors represent a determinant and non-negligible element that must be addressed to ensure the effectiveness of cyber security measures. Effective strategies, established widely in the general research stream of Risk Management, highlight the first way to build best practices in cybersecurity. To proceed with the mitigation strategies inferred from existing literature, it is useful to categorize only those action strategies. As proposed by[39], the risk quantification approach can take inspiration from the various literature sources that identify risk as a function of potential threats, vulnerabilities, and consequences[40,41]. Threats, represented by the internal or external agents intended to disrupt or cause harm to the organization, is the least manageable factor for organizations; therefore, this area of intervention is less relevant for the overall mitigation of cyber risk when compared to the two other factors. Nevertheless, managers can try to mitigate internal threats through different strategies: (1) Background checks of personnel, (2) Operating policies and procedures, and (3) Quality control procedures. On the other hand, regarding external agent threats, as it is impossible to clearly identify ex-ante such agents and affect them, means to mitigate, or eliminate this type of threat are generally absent. Vulnerabilities, defined as a weakness in the system that can be exploited by criminals, are one of the two other parts of the risk equation that are relatively easy to address by managers. In this contest, the most known mitigation strategies within risk management take place. Generally, such mitigations actions are connected to the probability of occurrence (and success) of a cyber-attack: Education of employees' cyber awareness, Enforcement of cyber security policy, Strong password policy, Multifactor authentication, Enact encryption, Regular updating of firewalls, virus scanners, intrusion detection systems[42], Updated inventory of systems, devices, software, services and IT applications in use, Identification of specific responsible person for management and protection of information and computer systems, Use of always-updated technical software. Consequences, i.e. the result on the system if the threat has successfully exploited vulnerabilities, represent the other factor that managers can address in a targeted manner. Mitigation actions linked to risk consequences are generally about lowering the negative impact of cyber-attacks once they succeed in breaching or are ready and able to damage the organization: Keep supervisory control networks and

39. M. HENRIE, Cyber Security Risk Management in the SCADA Critical Infrastructure Environment, Https://Doi.Org/10.1080/10429247.2013.11431973. 25 (2015) pp. 38–45.

40. A. TERRY BAHILL, E.D. SMITH, An Industry Standard Risk Analysis Technique, Http://Dx.Doi.Org/10.1080/10429247.2009.11431841. 21 (2015) pp. 16–29.

41. R. PATIL, K. GRANTHAM, D. STEELE, Business Risk in Early Design: A Business Risk Assessment Approach, Http://Dx.Doi.Org/10.1080/10429247.2012.11431927. 24 (2015) pp. 35–46.

corporate networks separate[42], Hunt for intrusions, Creation of a System Recovery Plan, Periodic backups of business-critical information and data, Clear and widespread procedures to inform cybersecurity personnel in case of attack.
A possible complementary solution, to help build best practices from the above Risk Management strategies, is to rely on the increasing development, by organizations, of digitalization capabilities that can have a direct impact on securing business solutions and organizational resilience as well[3,43]. Among the most relevant solutions emerging from the literature, the organizations may use a variety of heterogeneous resources to implement digital solutions at varying degrees and stages throughout business operations.
This strategy may involve differentiating between digitalization capabilities that enable information exchange and processing, and those that facilitate task automation[44]. Building improvisational capabilities, both at an organizational and individual level appeared to be another key element. We refer to these as capabilities that allow for impromptu adaptation and are most suitable for highly volatile environments that are defined by abrupt shifts in demand and unforeseen technological advancements[45].
From a more detailed perspective, these can be seen as the ability to quickly modify current resources and create new operational capabilities in response to unforeseen and pressing environmental circumstances using IT-based capabilities, such as the efficient utilization of digital IT systems[46].
Following this line of thought, the timely reconfiguration of resources can also be seen as a distinctive capability on its own[47]. However, the digitalization capability that can be seen as the most immediate and relevant refers to promoting a continuous learning environment: organizations ought to encourage ongoing education regarding the distinct features of digital technologies, by obtaining fresh expertise from both internal and external sources, and by establishing novel digital roles[47].

42. C. TAYLOR, P. OMAN, A. KRINGS, Assessing Power Substation Network Security and Survivability: A Work in Progress Report, (2003).
43. A. ANNARELLI, F. NONINO, G. PALOMBI, Understanding the management of cyber resilient systems, Comput Ind Eng. 149 (2020) pp. 106829.
44. P.L. DRNEVICH, D.C. CROSON, Information technology and business-level strategy: Toward an integrated theoretical perspective, MIS Q. 37 (2013) pp. 483–509.
45. O.A. EL SAWY, A. MALHOTRA, Y.K. PARK, P.A. PAVLOU, Research Commentary—Seeking the Configurations of Digital Ecodynamics: It Takes Three to Tango, Https://Doi.Org/10.1287/Isre.1100.0326. 21 (2010) pp. 835–848.
46. B.C. WHEELER, Identifying the organizational in NEBIC theory's choosing capability, 36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of The. 13 (2003) pp. 125–146.
47. D. NYLÉN, J. HOLMSTRÖM, Digital innovation strategy: A framework for diagnosing and improving digital product and service innovation, Bus Horiz. 58 (2015) pp. 57–67.

Conclusion

This paper aimed to discuss the impact of human factors in the context of cyber security management, while suggesting possible ways to effectively manage it, also following principles derived from the Risk Management perspective. Managing cybersecurity is a complex activity with multiple actors and systems involved. This research presents a model, the multi-layer attack graph, capable of capturing this complexity and managing increasingly sophisticated cyber threats. The proposed model not only maps threats from a technical point of view by studying the relationships between known access layers and network layers but stresses the importance of including a human layer in the assessments. However, in order to include the human dimension one must formalize what characterizes the individual in the human layer.

To this extent, there is a certain degree of acknowledgment of these factors and their severity from both practitioners and scholars, proven by multiple efforts towards categorizing them [13] but still a systematic development of knowledge on human factors and human vulnerabilities lacks.

The article proposed an initial classification of human factors involved in cyber security representing a starting point in constructing the relationship between human factors, human behaviors and cybersecurity vulnerabilities. Finally, the article stressed the importance of identifying strategies that can leverage human capabilities for an effective cybersecurity process. In conclusion, the study proposed an approach that can help the practitioners to think in a cybersecurity perspective that does not only focus on technical aspects but also considers as important the human element with all its peculiarities that make it both a vulnerability and a possible mitigation factor.

Possible future directions include the development of a comprehensive taxonomy of these factors, involving researchers and experts in the field in its formulation. Next, a semi-quantitative methodology will be investigated to define a cybersecurity profile of individuals to characterize the function that links the nodes of the model.

Finally, efforts should also be made to identify and evaluate possible solutions, such as proposed risk mitigation factors and digitization capabilities.