Importance of Human Factors on Cybersecurity within Organizations

A Study of Attitudes and Behaviors

Elham Rajabian Noghondar
Data Center
Tamin ICT& Management Consultancy
Tehran, Iran
Elham.rajabian@hotmail.com

***Abstract*—The rise of cybersecurity incidents is a threat to most organizations, while the impact of the incidents is unique for each of the organizations. There is a requirement to create the right conditions which provide rhythm to cybersecurity growth and a fully developed cybersecurity resilience. Having a mindset of cybersecurity resilience works actively to adapt people, processes and technology. Meanwhile, the adequate cultural cybersecurity conditions need to be achieved. It seems necessary to employ behavioral sciences to concentrate on employees' behavior in order to achieve concrete security mitigation preparedness regarding cybersecurity incidents. There are noticeable differences among users of a computer system in terms of complying with security behavior. The people differences can be studied under several headings, such as delaying tactics on something that must be done, the tendency to act without thinking, future thinking about unexpected implications of present-day issues, and risk-taking behaviors in security policy compliance. In this article, we introduce high profile cyber-attacks and their impacts on weakening cyber resilience in organizations. We also give attention to human errors and behaviors that weaken general security readiness in organizations. The human errors are discussed as a part of psychological matters to enhance compliance with security policy.**

Keywords-cyber resilience, human factors, cybersecurity behavior, attitude, usability, security culture

I. INTRODUCTION

In a world of continuous change, addressing cyber risks within organizations is already a huge leadership challenge. Regardless of organization size, it is critically important that each organization develops its own cyber crisis preparation response plan. Moreover, having a cyber-resilience approach in place prohibits a serious financial and reputational harm to organizations and their leaders.

Digital, dynamic and complex workplaces are great targets for cyber-criminals [1]. Cyber-criminal actors are people who search for any chance to steal data, blocking access with ransomware, or install evasive malware to remain undetected for long-term malicious effect. They utilize security breaches that emerge from weak links in, for instance, embedded software and applications in organization environment. Hence, technology and tools alone are not the answer for the cyber risks; after all, we have not seen the high- profile breaches in the headlines. In addition, the nature of attacks has altered from theft to become more harmful than ever since the threats become more complicated and harder to recognize. For instance, current attack scenarios target backup data repositories and administrator functions, which are the last lines of defense in organizations [5].

The two main high-profile cyber-attacks in 2021 involved confidential data lost and various forms of ransomware attacks. Confidential data was stolen from large organizations like Singtel, the University of Colorado, Aerospace Company Bombardier and the Australian Securities and Investments Commission. Moreover, various types of ransomware attacks have occurred in organizations such as Acer Company, United States CAN Insurance, Scotland's University of the Highlands, United States Colonial Pipeline, California Water and Wastewater System, etc. Furthermore, based on the GDATA news in 2021, the most recognized type of security attacks include phishing, clever ransomware, polyglot files, IoT attacks, social engineering, malvertising on Facebook feeds, identity theft, password and data breach, zero-day exploits, insider threats and deep fake attacks.

Organizations with integrated information technology systems and operational technology systems propose clear and unclear points of convergence that directly threaten functionality of the technical systems [2] [3], like the attack against the Water and Wastewater System in California. The attacks usually work against the four main functions of information communications technology systems: quality and efficiency of services, data confidentiality, improved usability and people privacy and safety.

Organizations need awareness about immaturity in their risk mitigation measures. They also should recognize depth of threats that result from insiders at the same time [4]. We believe that insiders' threats are becoming more frequent, as they are difficult to detect and insiders already have legitimate access to the network infrastructure [4]. In addition, variety in embedded applications is a source of data leakage [5]. The growth in the amount of stored data widens the cyber-attack surface. Transition to cloud computing technologies poses major difficulties in identifying insider attacks as well [6]. Because of all the mentioned complexities, such as immature risk mitigation measures, the role of insiders, difficulty in recognizing threats from insiders to a wide range of embedded software and business applications, stored data growth and cloud data repositories, more research is needed in order to enhance organizational resilience. In this article, we aim to discuss how a people-centric approach in parallel with a technology-centric approach can largely mitigate cybersecurity risks in organizations. We also investigate how cyber resilience limits the scope of cybercrime within organizations. The research methodology is a qualitative method based on systematic literature study along with case studies that prove the importance of human factors in cybersecurity. The case studies are used to shape discussions, to locate gaps and draw conclusions. The organizational challenges are studied to shape a sustainable cyber risk management approach in the related work section. Insider behaviors are viewed as a cybersecurity gap to draw proper cyber resilience in Section 3. The challenges to perform the best cybersecurity practices are mentioned in Section 4. Some guidelines and metrics are provided to measure cyber resilience in organizations in Section 5. At the end, we indicate some points to build a cybersecurity culture based on individual behavior.

II. RELATED WORK

Sometimes organizations encounter problems to manage cyber risks and develop a sustainable security framework. They don’t pay enough attention to knowledge, guidance and research for the technologies’ innovations. In addition, there are no incentives like market forces and no regulation for utilizing the emerging technologies in a secure manner [7]. A sustainable security framework should mitigate the issues such as skills gaps, fragmented security approaches, obscure liabilities in cyber resilience, lack of operational security capabilities and lack of technical solutions in responding to incidents.

Organizations face a competitive market and they are concerned about the sustainability of their operations from economic, environmental and social viewpoints. This is called the sustainability of business. It means that business strategy and competitiveness don’t necessarily interfere with sustainability of environment and society [8]. On the other hand, digitalization also brings complexity in cyber space and organizations are exposed to cyber threats as a result [9]. Therefore, organizations need to understand cyber resilience as an ability to plan ahead, to respond, to recover from and adapt to the cyber threats.

Cyber resilience can be achieved through a secure information infrastructure and a proactive workforce that takes both the human factor and the organizational factor serious simultaneously. Based on our organizational experience, there are many opportunities for purchasing technical devices to get ready against cybersecurity attacks. Many organizations have cybersecurity risks at their core due to untuned embedded devices and other negligent factors. Moreover, during the last few years, there is noticeable attention to the human side of the cyber risk but there is still growth in data breach and other human-related threats [5]. One reason to consider just objective activities and pay too little attention to people and their behavioral aspect. In addition to this, there is a lack of proper policies and of procedures to encourage the desired human behavior. These are the main reasons why current cybersecurity solutions are not effective.

To specify security problems, besides the above issues, organizations should also keep an eye on the numerous technological transformations intended to enhance profitability, and consider them in their security checklists. Most such transformations have potential to generate new systemic risks [11]. Examples are artificial intelligence and advanced machine learning [6], ubiquitous connectivity, quantum computing solutions and next-generation digital identity systems [11]. Append to these the current cybersecurity problems such as distributed cloud-based infrastructure, integrating software, web applications that reside on premises behind firewalls, etc. [7]. Some organizations set policies, standards, apply the best security practices and make partnership to avert such cybersecurity threats. In addition, organizations need to share and develop research, insights and solutions to manage the future-risks as a community. At the same time, there is a need for adopting a defense-in-depth security strategy with the aim of receiving perfect cooperation from the main fundamental cybersecurity components including people, processes and technology [13]. We contribute with an analysis of different incidents and threats reports to show that current cybersecurity breaches are the result of too little attention to human factors and too much focus on tech-centric solutions. We collect the latest cybersecurity reports and study the cause and effect for each incident. In addition, the components of cyber resilience strategy and corresponding metrics are discussed as a limitation for cybercrime impacts. We also introduce a cybersecurity training scheme for employees’ preparation to recognize the signs of malicious activity in advance. We carry out pillars for cybersecurity culture and the desired behavioral pattern toward a well-structured cybersecurity culture as well.

III. THE CYBERSECURITY AND HUMAN FACTOR

As we mentioned earlier, organizations usually display great progress to employ different technical security solutions such as firewalls, virus scanners, web application firewalls and intrusion detection systems to control the potential cybersecurity threats [14]. This happens because CIS normally recommend a technology-centric approach with little emphasis on human factors, needs and motivations [15]. But there is a demand for a holistic security approach, as technical solutions merely cannot handle cybersecurity attacks. This is the way to acquire cyber resilience. Thus, we have to discuss insiders’ threats besides the threats related to the information infrastructure and the processes. Insiders are the individuals who have access to resources, detailed knowledge about the computer network infrastructure, and data storage technical infrastructure. They include staff, contractors, partners, vendors and other stakeholders [16]. Insiders usually are aware of the location of sensitive data, what protective measures are in place, such as firewalls and the designed security policies. They often know of cybersecurity concerns and bottlenecks. They also have capabilities and skills to conceal the crime footprint for a long time or sometime forever [17]. Therefore, insiders present much more danger with potentially higher damage than external cyberattacks.

According to Data Breach Investigations Report in 2021, insiders are in charge of 22% of security incidents. Furthermore, based on Stanford University, around 88% of data breaches are caused by staff mistakes. Bitglass [49] report in 2022 revealed that top insider actors of security incidents are privileged users and administrators (63%), privileged business users and C-level executives with access to sensitive data (60%), third parties and temporary workers such as contractors and consultants (57%) and regular employees (51%) as shown in Fig. 1.

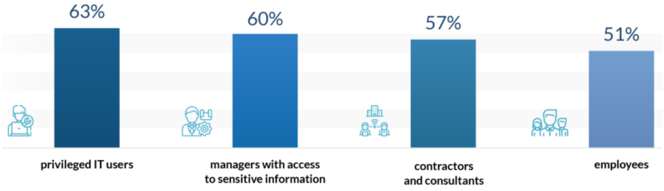

Figure 1. Top Insider Threat Actors in 2022.

Moreover, 62% of the security incidents result from negligent employees or contractors while 14% of the incidents were caused by malicious insiders, according to Panda security report in 2020 [18].

Fortinet [47] described that the most prevalent type of insider threats is phishing, about 38% in 2019. For instance, exploitation of insecure RDP, and unsupported or outdated operating systems and software result in the phishing attack. Moreover, according to US Securonix [48] report in 2020, the most frequent cyber incidents include data extrusion accounting for 62%, privilege misuse about 19%, data snooping for 9.5%, infrastructure sabotage around 5% and circumvention of IT controls for 3.8%. Fortinet also defines fraud as the primary motivation behind insider threats around 55%, monetary gain for 49% and IP theft for 44% in 2019. The most frequent types of attacks related to human factor involve online fraud like phishing, DDOS, ransomware and social engineering [20]-[23]. Fig.2, displays stop motivations for insider attacks.

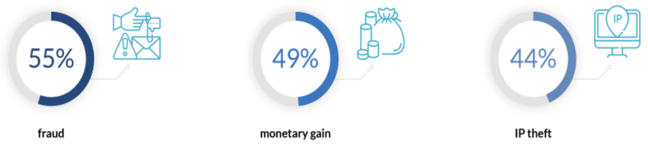

Figure 2. Top Motivations for Insider Attacks.

For several reasons, finding solutions for the insider threats is even more difficult than implementing measures to protect against foreign and external threats. Most companies and organizations rely on security awareness training, followed by company policies, procedures and intelligent automation to protect themselves against the insider threats. Ironically most employees say they understand the company policies and the procedures. Comprehension does not help to prevent incidents due to malicious behavior or negligence. The early indicators of such actions distribute themselves across vast data silo repositories that historically defied our ability to wrap our cognitively limited minds around [17]. To reduce the cyber risk gaps organizations' top managers need to learn about threats by implementing a mature cybersecurity risk management. They need to consider one key lesson: while technical upgrades are important, minimizing human errors by studying employees' attitudes is even more vital. Mistakes by network administrators and users' failures to patch vulnerabilities in legacy systems, misconfigured settings, violations of standard procedures-open the door to the overwhelming majority of successful attacks [23]. To flourish, they should move beyond protection to resilience.

IV. THE CHALLENGES TO CYBERSECURITY PRACTICES

Hidden interconnections among organizational factors affect the quality of services provided by organizations. They may influence in individual's total performance and their actions. For example, poorly written rules, faulty equipment, web application misconfiguration, poor management practices and vague procedures [24] [25]. These refer to more breaches and create consequences that are more adverse. There are four discussable CIS challenges in path of implementing cybersecurity best practices and attack mitigation in organizations. They include individual factors, organizational factors, technological factors and ethical matters [26].

When we talk about the individual factor, it is about inadequate security actions causing both errors and/or violations. Incorrect configurations of work elements will cause unintentional errors and conscious actions of non-malicious attempts [27]. The theory of Reasoned Action [19] and the theory of Planned Behavior discuss two solid models that link behaviors and attitudes. It is about an indirect psychological connection that is called "behavioral intention" [27]. It makes clear that there is a feasibility to define human failures and violations via studying staffs' attitudes versus cybersecurity critical behaviors. Reasonably, cybersecurity behaviors can directly predict attitudes and the exact behavioral purpose of high-risk behaviors. Thus, it is important to understand the relation between attitudes and deliberate actions in order to avoid the CIS breaches [17]. Furthermore, to enhance the cybersecurity situation, there is a need to set bases to form attitudes like subjective norms and beliefs to perceive consequences of an action, acquire actual knowledge about the cybersecurity matter, the cognitive strategies utilized in decision-making process, etc. Staff attitudes can also encourage the impact of social and organizational factors. For instance, social norms, ethical dilemmas, and different levels of behavioral control understood by staff members such as the degree of freedom taken in to display a given behavior and contextual enablers in place, are connected to such given behavior [27]. There are psychological frameworks that can be applied with the aim of reducing the security violations and giving emphasis to the role of norms and the ethical values informing staff attitudes. The Norm Activation Theory [37], makes clear that attitudes are certainly impressed by the moral obligation levels, self-responsibility and clear awareness about emerging consequences of a given behavior [27]. Employees' awareness and training downgrade the probability of sudden and unintentional behaviors which cause a violation from cybersecurity rules. In consequence, it largely minimizes the information security risks and preserves the important organizational assets and the intellectual property [28]. Therefore, perceiving the tiny differences between human errors and violations specifies organizational bottleneck points. In addition, building an information security culture based on behavioral issues, and incorporate the created culture framework into organizational levels contribute towards reducing the risk from employees' behavioral fault and related human errors.

The second discussable cybersecurity challenge is the organizational factor. Many organizations proceed towards mitigating the cyber security vulnerabilities by forming policies, processes and procedures. Although the organizations require their employees' compliance with the regulations and the procedures, the formal regulations merely do not construct the desired human behavior [29] [33]. For instance, the complex architecture of computer networks, resources and data storage infrastructure provide possibility for individuals to use the system in unprotected modes, pretending as a usual and useful activity [18]. Deviating from security practices can occur because informal procedures and intuitional cost-benefit estimations override potential negative results of one's activity. For example, passwords are written down or shared with colleagues. Therefore, employees will not follow the organizational policies and rules if they are too costly or it is unclear how to implement them [27] [30].

The third imaginative challenge is the technological factor. In this regard, CIS supplies an effective and useable security design. Users certainly refuse security mechanisms that are hard to utilize or cause faults that weaken security [32]. Usability is a degree of effectiveness, efficiency, and satisfaction with which users of a system can recognize predesignate tasks. Low usability may directly threaten safety, quality and efficiency, especially when it leads to human errors and slows down organizational processes. Inadequate usability might cause indirect cybersecurity risks. For example, when aggressive warning notifications encourage users to deactivate the security notifications [34]. In addition, it is difficult to integrate employees' differences and socio-cultural variables without a usable security design [35]. To improve usability, the security principles should be user-experience based. This is still a real issue with the CIS implementation in organizations. Weak usability in the security design leads to improper operation of cybersecurity tools and poor functionality. It ultimately creates in-effectiveness [31]. A unified user interface for various user domains may solve some usability and acceptability related issues [36]. Therefore, giving priority to the user interface design and good user experience leads to positive attitudes and facilitates the usage of procedures, software and applications [27].

The fourth challenge, ethical matter is discussable under role of the norms in shaping employee's attitude based on the Norm Activation Theory. In other words, employees' attitude is directly impressed by moral obligation, the ethical norms, and their clear knowledge about the consequences of a particular behavior [37]. In collective actions, individual efforts are negligible when others do not perform their role as desired. Thus, having information about others behavior supplies clear overview about behavioral norms, which have an independent influence on behavior [38].

V. CYBER RESILIENCE OVER CYBERSECURITY

Cyber resilience should restrict the impact of cybercrime in organizations, business brand reputation, financial commitment, legal, and customer trust obligations. These areas demand resources and executive support, as they are important subjects in case of an actual threat [39]. In other words, cyber resilience should bring a certain level of confidence for business continuity and ability to respond to security attacks with purpose of preserving the obligations [40]. Fig. 3 illustrates the relationship between cyber resilience, crisis management and reconstruction.

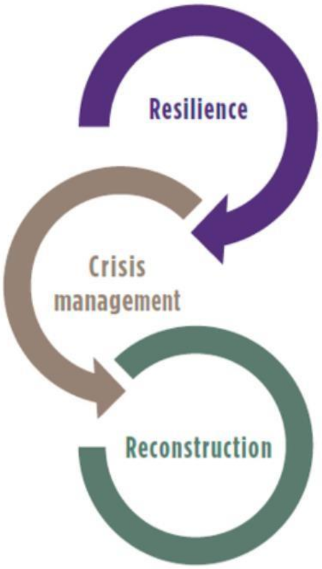

Figure 3. Cyber Resilience Crisis Management and Reconstruction.

Cyber resilience should present some cybersecurity basis such as patching vulnerabilities, detecting and lessening threats, and training programs for employees on how to defend their organization's security [41]. It is about a continuous functionality not a yearly action as well. In addition, the cyber resilience idea must build into each part of the organizational departments, from business process mapping to service availability engineering to critical stakeholder and vendor dependency [42]. Fig. 4 presents components of a cyber-resilience strategy:

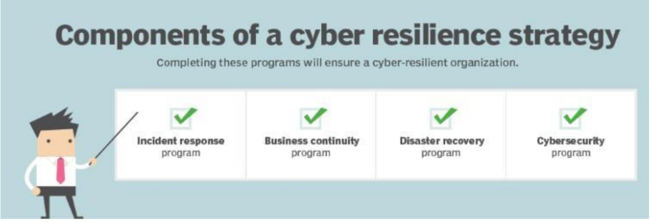
Components of a cyber resilience strategy
Completing these programs will ensure a cyber-resilient organization.
Incident response program
Business continuity program
Disaster recovery program
Cybersecurity program

Figure 4. Components of Cyber Resilience Strategy.

Currently, there is a demand for a mature cyber resilience framework and specific metrics to measure cyber resilience. The mature cyber resilience framework must propose a set of features including quick response and recovery procedures in minimal time in case of an incident while supporting organizational priorities [43]. The cyber resilience framework helps leaders to understand what cyber resilience is and what attitudes can support the intended cyber resilience [16]. Organizations need to prioritize human-related solutions into their cyber resilience strategy for workforces. Cyber resilience is not about comparison, and there is no final destination. It is about a measurement framework that scales businesses by focusing on people, processes and technology to make sure that entire value chains are resilient while adopting the desired security culture [39].

The training program should empower staff to actively consider cyber risk. Employees require to be trained about different possible security layers. As nowadays the most common attacks are again web applications they ought to know about the most popular web vulnerabilities and the impacts. For instance, phishing, social engineering, password-based attacks, injection attacks, information leakage, email attacks, malware attacks, ransomware, DDOS, etc. In addition, the role of insiders should be part of the cybersecurity training scheme. To follow up the effectiveness of the training package, random testing of employees should be performed. For example, a test email including malware can be sent to employees and their responses are evaluated. Therefore, it is an appropriate measure to undertake further education. CEO should have an active role in forming an impressive cyber training program. CEO not only has authority to create the overall cybersecurity strategy but also can supply executive guarantee for the strategy. It also helps staff to understand the significance of the training programs. The other C-suite members like CIO, or CISO bear primary accountability for implementing the educating procedures. In this manner, we take steps in building a culture of cybersecurity and increase cyber resilience in the organization. Furthermore, expanding monitoring capabilities and knowledge should be trained with the aim of receiving better cyber resilience performance.

A. Measuring Cyber Resilience

It should be an ultimate mission for organizations to concentrate on their cyber resilience capabilities and the actual influences emerging from the technical and the organizational security measures in order to evaluate the cybersecurity posture [44]. In other words, measuring and quantifying the state of cyber resilience are essential because leaders decide about additional security measures.

Traditional security metrics restrict vision about the real performance of cyber resilience provisions as they merely pay attention to existing security controls or completion of particular security necessities [45]. For instance, sometimes organizations measure the state of security awareness among employees through evaluating participation on mandatory security training course. However, completing an E-learning module will not necessarily assure to behave proper in case of a real security threat [46]. To correct such loss in the traditional security metrics model, some ability-metrics are needed to assess outcome of cyber resilience performance. A meaningful cyber resilience metrics model argues a spectrum of metrics includes ability to avert social engineering, ability to engage threat intelligence, ability to address vulnerabilities, ability to handle cyber incidents, ability to resist malware, ability to resist system intrusions, ability to resist DDoS attacks, ability to protect credentials, ability to protect key assets and ability to measure and minimize damage [9], and ability to assess insider threats. We believe in the predominance of evaluating the metrics model versus actually occurred attack scenarios in different industries, to check the degree of the avert ability in various stages of the attacks.

Each organization indicates its unique security risks. Therefore, there is no unique cyber resilience model which fits all imaginable features of risk [10]. Based on the described opinion above and in the literature, measuring cyber resilience can be accomplished by the following core guidelines with the aim of finding the breaches faster, fixing them faster and minimize their impact:

- Provide a centralized asset management system. Specify organizational valuable possession including hardware, software and data. Isolate backup data. Recognize critical potentialities that may act against the asset and the demanded organizational cyber resilience.
- Define the interlinkage between the organizational systems and find out how the interconnectivity makes the system vulnerable versus the actual attack scenarios. In this regard, ensure proper security monitoring for the organizational perimeter.
- Recognize the organizational characteristics, current organizational cyber resilience attitude; partner with peers, competitors and public entities to emphasize threat intelligence sharing among the organizational networks.
- Consider people hiring cycle and how to develop people’s skills & behavior. Effective cyber resilience needs a strong cultural concentration driven by the organization’s board and C-level management which reflects in the organization via wide programs to educate and increase cyber awareness of staff and third parties.
- Measure towards a culture of trust, organizational agility and continue to stakeholders trust and transparency at the same time.

VI. BUILDING CYBERSECUIRTY CULTURE BASED ON BEHAVIOR

Cybersecurity empowers organizational objectives and progressively provides competitive benefit [41]. Security culture is a set of security-based norms, values, attitudes and obligations within an organization. It especially focuses on the human related matters. Security culture adds value by evaluating shared opinions, customs, social behavior, adequate investment and management instruction for cybersecurity [15]. Improving security culture increases organizations security readiness [39]. It is a fact that the security culture is built top down. Building and maintaining a security culture notably leads to a higher security awareness among employees. As a result, employees will naturally behave as a proactive protective layer. It means, more attention to security culture gives greater likelihood that employees follow the security practices and consequently behave more securely. It finally causes overall reduction in the organizational risks. In general security culture is influenced by seven main dimensions: attitude, behavior, cognition, communication, compliance, norms and responsibility [41].

Attitude describes the feelings and beliefs that individuals propose to security protocols and security issues [14] [41]. Behavior refers to all activities of employees that have direct and indirect impact on security issues within an organization [40]. Behavior is defined as the combination of actions and habits in a situation, environment or stimulus [12]. Cognition discusses awareness, knowledge and employees' understanding of the security issues and related activities. Communication is about the quality of communication channels to share cybersecurity events, news and analysis of the security-related subjects. It encourages a real sense of belonging and helps solve security problems and incident reporting [41]. In a well-structured cybersecurity culture, leadership communicates the organizational security principles which should not be violated. These include procedural compliance, questioning attitude, integrity compliance, depth of knowledge, forceful backup and formality [23]. Compliance ensures knowledge about written security policies and determines security policies' scope which must be followed by employees. Norms talk about knowledge and commitment to unwritten management rules in organizations. Responsibility makes explicit how employees understand the significance of their role in supporting or threatening the security of their organization [41].

In constructing cybersecurity culture based on insiders' behavior, leadership also should train employees to listen to the internal alarms, search for causes and take right action. In addition, leadership should encourage procedural compliance and a questioning attitude among staff [15]. Employees with a questioning attitude usually perform double-and triple-check work, keep notifying for anomalies, and are never pleased with a less-than-complete response [23]. Moreover, compromising behavior which leads to security breaches, usually means breaches in the security principles [15]. For instance, imagine a system admin with fewer access limitations surfing the web and downloading an infected video clip. It clearly violates integrity and the procedural compliance. An employee who clicks on a malicious emailed link during online shopping is in phishing danger. It indicates lack of a questioning attitude, depth of knowledge and lack of procedural compliance. A beginner network administrator installs an update without consulting the implementation guide and with no supervision. Therefore, the former security upgrades are unpatched. In this case, depth of knowledge, procedural compliance, and forceful backup causes the problem. Think about a network help desk that resets a connection without exploring the reason for the deactivation. It might be an automated shutdown to prohibit an unauthorized access. It is again a type of breaking procedural compliance and a questioning attitude [23].

There is no conclusive method to establish a concrete cybersecurity culture but working actively on the behavior changing process. To achieve it, top-level management should specify the desired behavioral pattern and formulate how to reach goals and implement them. Improving security culture definitely provides more secure behavior from staffs' side. It consequently mitigates the general risks statistics within organizations. Below, we supply some points that can be beneficial in the way of improving the security culture into organizations:

- Set up periodic risk assessment and an ongoing monitoring solution for early discovering the organizational risks. Define human factor a serious matter in the risk assessment procedure.
- Define a human-related ability metric in the organizational cyber resilience metrics model. Measure the individuals' awareness and behavior with it.
- Expand a security-awareness culture; make aware employees about the desired behavior, unpleasant consequences and their responsibility in lack of compliance. Shape a strong security culture scheme by use of the seven main effective dimensions: attitude, behavior, cognition, communication, compliance, norms and responsibility.
- Create a positive cybersecurity culture by involving psychological methods into the security culture scheme, using novel "polymorphic" security warnings, rewarding and penalizing desired and undesired cyber behavior.
- Deploy automated awareness-training programs for a varied audience including all organizational departments and use unified communication tools and attack simulations. Define core organizational values and communicate the security-related leadership instructions clearly in a prescribed manner in a proper atmosphere without side descriptions which lead to inattention, faulty assumption and other errors.
- Take advantage of an analytical-driven security strategy by mobilizing an active messaging program across the organization, and develop a security community with peers to share knowledge and learn from them.

VII. Conclusion and Future Work

The contribution of the paper resides in the multi-factoring CIS challenges to prevent the cybersecurity attacks in organizations, with a special focus on the complexity of human factors. To manage cybersecurity risks, it is inevitable promoting a people- and technology-centric comprehensive approach in organizations. We specify the importance of differentiating human errors and violations based on the individuals' attitudes and characteristics. In this manner, we highlight the significance of the interdependency among organizational components which may affect employees' general performance and actions. Improving cybersecurity culture is the main mission in this paper. We discuss how cybersecurity culture can increase organizations' cybersecurity readiness. We highlight the seven main components to improve a security culture model: attitude, behavior, cognition, communication, compliance, norms and responsibility. Thus, employees naturally behave as a proactive protective layer as defined in the cybersecurity culture model. The human-centric approach leads to overall reduction of cybersecurity risks in parallel with the technology-centric approach. As a result, cybersecurity resilience seriously restricts the scope of cybercrime in organizations. A mature cyber security resilience framework should include some ability-metrics for evaluation of the cybersecurity resilience performance. Future research could continue to explore the desired human behaviors that improve cybersecurity culture and accordingly form proper cybersecurity resilience. In addition, it should be investigated how an organization can achieve the desired behaviors from individuals.

References

[1] Gregory Vial, Understanding digital transformation: A review and a research agenda, pp.4, 2019, https://doi.org/10.1016/j.jsis.2019.01.003.

[2] Patrick Katuruza, IT-OT Convergence: Managing the Cybersecurity Risks, 2021. Available from:https://gca.isa.org/blog/it-ot-convergence-managing-the-cybersecurity-risks.

[3] Richard Paes, David C Mazur, and Bruce K. Venne, A Guide to Securing Industrial Control Networks -IT/OT Convergence ,IEEE, Dec. 2019, pp.49-50. Electronic ISSN:1558-0598, https://doi.org/10.1109/MIAS.2019.2943630.

[4] Cybersecurity and Infrastructure Security Agency CISA, Insider Threat Mitigation Guide, pp. 20-21,2020.

[5] EU Data Protection Board, Examples Regarding Personal Data Breach Notification, pp. 15-16,2021.

[6] Pupillo Lorenzo, Fantin Stefano, Afonso Ferreira, and Polito Carolina, Artificial Intelligence and Cybersecurity Technology, Governance and Policy Challenges, pp. 40-41,2021.

[7] World Economic Forum with collaboration with Oxford University, Cybersecurity, Emerging Technology and Systemic Risk, pp. 44,2020.

[8] Alessandro Annarelli and Giulia Palombi, Digitalization Capabilities for Sustainable Cyber Resilience: A Conceptual Framework, pp.6,2021. https://doi.org/10.3390/su132313065.

[9] Participants in the Cyber Security Shared Research Program, Library of Cyber Resilience Metrics, pp.10,2017.

[10] Jim Alkove, Cyber security is no longer enough: businesses need cyber resilience, Available From:https://www.weforum.org/agenda/2021/11/why-move-cybersecurity-to-cyber-resilience/2021.

[11] Yuchong Liand Qinghui Liu, A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments, pp. 7-8, 2021.https://doi.org/10.1016/j.egyr.2021.08.126

[12] Keri Pearlson, Sean Sposito, Masha Arbismanand Josh A.Schwartz, How Yahoo Built a Culture of Cybersecurity,2021.

[13] Sivaram Chelakkara, CEH, CISSP, and GCISP, People, Processand Technology in Cybersecurity, pp. 4-6,2020.

[14] Check Point Software, Cyber Attack Trends, pp. 21-24,2021.

[15] Stjepan Groš, A Critical View on CIS Controls, pp. 3-5,2019.

[16] Nena Giandomenico and Juliana de Groot, Insider vs. Outsider Data Security Threats: What is the Greater Risk?, Available from:https://digitalguardian.com/blog/insider-outsider-data-security-threats,2020.

[17] Neetesh Saxena, Emma Hayes, Elisa Bertino, and Patrick Ojo, Impact and Key Challenges of Insider Threats on Organizations and Critical Businesses, pp. 16-17, 2020.doi:10.3390/electronics9091460

[18] Danny Murphy, Insider Threat Statistics, pp.6,2021.

[19] Martin Fishbein and Icek Ajzen, The Theory of Reasoned Actionof Fishbein and Ajzen, pp. 7-8,1975.

[20] Icek Ajzen, The Theory of Planned Behaviour, 1991.

[21] Regner Sabillon, Jeimy J. Cano M, Jordi Serra Ruiz, and Victor Cavaller, Cybercriminals, cyberattacks and cybercrime, pp.8,2016.

[22] Michael Swanagan, CISSO, CISA and CISM, Cyber Security Statistics The Ultimate List of Stats Data and Trends, pp.9,2022.

[23] Tashfiq Rahman, Rohani Rohan, Debajyoti Pal, and Prasert Kanthamanon, Human Factors in Cybersecurity: A Scoping Reviewpp. 8-9, 2021.doi:10.1145/3468784.3468789

[24] Alessandro Pollinietal, Leveraging human factors in cybersecurity: an integrated methodological approach, pp 11,2021.

[25] Edward Staddon, Valeria Loscri and Nathalie Mitton, Attack Categorisation for IoT Applications in Critical Infrastructures, pp. 14, 2021.https://doi.org/10.3390/app11167228.

[26] Moti Zwilling, Trends and Challenges Regarding Cyber Risk Mitigation by CISOs, A Systematic Literature and Experts' Opinion Review Based on Text Analytics, pp. 7,2022.

[27] Jongkil Jay Jeong, Joanne Mihelcic, Gillian Christina Oliver,andCarsten Rudolph, Towards an Improved Understanding of Human Factors in Cybersecurity,pp. 5-6, 2019. doi:10.1109/CIC48465.2019.00047.

[28] Lee Hadlington, Employees Attitude towards Cyber Security and Risky Online Behaviours: An Empirical Assessment in the United Kingdom,pp. 9,2018.

[29] Kristina Gyllensten and Marianne Torner, Therole of organizational and social factors for information security in a nuclear power industry, pp. 10-11,2021.

[30] Rao Faizan Ali, Dhanapal Durai Dominic Panneer Selvam, Emad Azhar, and Mobashar Rehman, Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance,pp. 17, 2021.doi:10.3390/app11083383

[31] Rick Wash, Prioritizing Security over Usability: Strategies for how people choose passwords, pp. 8, 2021.https://doi.org/10.1093/cybsec/tyab012

[32] Angela Sasseand Ivan Flechais, Usable Security: Why Do We Need It? How Do We Get It? PP. 4-5, 2005.

[33] Sylwia Agata Beczkowska and Iwona Grabarek, The Importance of the Human Factor in Safety for the Transport of Dangerous Goods, pp.13, 2021.

[34] John Soldatos, Security Risk Management for The Internet of Things Technologies and Techniques for IOT Security, Privacy and Data Protection, pp. 35-37,2020.

[35] Sebastian Hengstler and Natalya Pryazhnykova, Reviewing the Interrelation Between Information Security and Culture, pp. 7,2021.

[36] Jing Wanget al., Research Trend of the Unified Theory of Acceptance and Use of Technology Theory: A Bibliometric Analysis, pp. 14, 2022. doi:10.3390/su14010010.

[37] Judith de Groot and Linda Steg, Morality and Prosocial Behavior: The Role of Awareness, Responsibility, and Norms in the Norm Activation Model, pp. 4, 2009.https://doi.org/10.3200/SOCP.149.4.425-449.

[38] Linda Steg and Judith de Groot, Explaining Prosocial Intentions: Testing causal relationships in the norm activation model, pp. 8, 2010. doi:10.1348/014466609X477745.

[39] Accenture Security, Innovate for Cyber Resilience, pp. 27,2020.

[40] DanielA.SepúlvedaEstay,RishikeshSahay,MichaelB.Barfod,andChristian D.Jensen, A systematic review of cyber-resilience assessment frameworks, pp. 9-10, 2020.doi:10.1016/j.cose.2020.101996.

[41] Javvad Malik, How Security Culture Invokes Secure Behaviour, Available from:https://www.infosecurity-magazine.com/blogs/security-culture-invokes-secure/,2021.

[42] Thomas H.Llansó, Daniel A.Hedgecock, and J.Aaron Pendergrass, The State of Cyber Resilience: Now and in the Future, pp. 4,2021.

[43] lessandro Annarelli and Giulia Palombi, Digitalization Capabilities for Sustainable CyberResilience,2021. pp.4,https://doi.org/10.3390/su132313065.

[44] Aviram Zrahia, Threat intelligence sharing between cybersecurity vendors: Network, dyadic, and agent views, pp. 6-7, 2018.https://doi.org/10.1093/cybsec/tyy008.

[45] Reinder Wolthuis, Shared Research Program Cyber Security, pp.11- 12,2021.

[46] McKinsey, Cybersecurity in a Digital Era, pp. 44, 2020.

[47] Fortinet, Insider Threat Report, pp. 5,2019.

[48] Securonix, Insider Threat Report, pp. 8,2020.

[49] Nestor Gilbert, 31 Crucial Insider Statistics Latest Threat and Challenges, pp. 3, 2022.