Development of Information Security Management in The Age of Remote Working

Māris Meļņikovs[1], Sarma Cakula[1]

[1]Faculty of Engineering, Vidzeme University of Applied Sciences, Valmiera, Latvia

Abstract.

Remote work has increasingly integrated into the daily routines of employees whose tasks are conducive to remote completion and do not necessitate physical presence at the workplace. This shift was particularly evident during the COVID-19 pandemic, wherein widespread restrictions compelled a substantial portion of the global workforce to operate remotely. However, this transition also unveiled vulnerabilities, notably in cybersecurity, as remote work setups often lacked the fortified network perimeters typical of physical office environments. This paper aims to augment the established "CIA Triad" supplementary components tailored to contemporary cybersecurity demands, particularly within the context of remote work arrangements organized by businesses. The researchers intend to examine existing alterations of the CIA triad put forth by various researchers and standards organizations. Through the assessment of these adaptations, they aim to enhance and expand upon the most comprehensive iteration of the CIA model by incorporating socio-technical elements to encompass the previously underemphasized facets of cybersecurity. Drawing upon insights from prior research, the researchers will identify the most suitable form of socio-technical model adjustments that comprehensively tackle cybersecurity challenges, particularly in bolstering the security posture of remote workers. Consequently, the researchers' newly developed model seeks to emphasize and fortify cybersecurity policies crucial to remote work environments, ultimately providing an optimal blend of strategies to enhance the security of remote teams.

Keywords: cybersecurity, information communication technologies, information security management systems, information security models, remote work.

1. Introduction

With the development of information technology and the increasing availability of the Internet, working remotely gained popularity among employees at the beginning of the 21st century (Babulak, 2009). The rise of remote work among professionals like accountants, engineers, recruiters, and sales managers was already gaining traction before the pandemic. However, the COVID-19 pandemic significantly accelerated this trend as global restrictions

necessitated widespread remote work adoption. This transition highlights the importance of protecting remote workers, especially in times of geopolitical tension such as Russia's actions in Ukraine and cyber-attacks on EU and NATO countries. Russia strategically employs cyber tactics to achieve geopolitical objectives, including asserting global status, controlling perceived spheres of influence, and destabilizing Western nations. The conflict in Ukraine has served as a testing ground for Russia's cyber warfare and disinformation strategies, showcasing their ongoing investment and refinement in cyber capabilities (Limnell, 2018). The EU, along with global partners, strongly condemns Russia's cyber attacks on Ukraine's KA-SAT satellite network before its invasion on February 24, 2022. These attacks caused widespread disruptions in Ukraine and affected EU Member States, highlighting Russia's irresponsible cyber behavior. Such actions violate UN standards and threaten the security of European citizens. (Council of the EU, 2022).

The analysis suggests that emphasizing legislation and regulatory frameworks is crucial in determining appropriate measures to mitigate risks and threats. Additionally, prioritizing employee training emerges as paramount within the realm of cybersecurity practices. Moreover, the emergence of novel social engineering trends underscores the need for vigilance, particularly in the context of expanded telecommuting. It's imperative to avoid viewing the widespread adoption of remote work solely as a crisis from a cybersecurity standpoint. Lastly, it's worth acknowledging that heightened awareness among employees regarding threats, risks, and best practices could paradoxically result in riskier behaviors, potentially endangering remote working organizations (Agnes Ekfors Elvin, 2021).

Companies had to make changes to their cybersecurity policies and infrastructure of Information and Communication Technology (ICT) and ensure secure off-premises staff and a secure network perimeter in a short time. Remote workers quickly became an easy target, as remote workers were in most cases more vulnerable to cyber-attacks than those inside the secure network perimeter of companies. With the development of this approach, the number of phishing e-mails sent, which were targeted specifically at company employees, increased rapidly. Contemporary security measures safeguard data from inexperienced cyber intruders such as script kiddies, yet they fail to effectively thwart the efforts of seasoned criminal hackers (Kowalski, 2011).

As the landscape of work evolves, driven by technological advancements and societal changes, it becomes imperative for chief executive officers (CEOs) to adapt their leadership styles and business processes accordingly. This adaptability is crucial for maintaining organizational efficiency and competitiveness in a dynamic environment. In the realm of cybersecurity, this paradigm shift presents a significant challenge for chief information security officers (CISOs), particularly concerning the security of remote work environments. Ensuring that remote workers, who operate outside the traditional confines of company premises, receive comparable levels of cybersecurity protection demands innovative strategies and robust infrastructural support. Achieving parity in security conditions between

remote and on-premises work environments necessitates a comprehensive understanding of evolving cyber threats, effective deployment of cybersecurity technologies, implementation of stringent access controls, and ongoing monitoring and assessment of security protocols. Addressing these challenges effectively not only safeguards sensitive organizational data but also fosters a culture of cybersecurity awareness and resilience across the workforce, ultimately contributing to sustained business continuity and success in today's digital age.

Before the pandemic, most companies' information security was governed by a "Castle-and-Moat approach" or "perimeter-based network security model". This model assumed that companies' users within the corporate network were "trusted" and everyone outside the corporate network perimeter was not trusted. In terms of remote work, the perimeter-based network security model is no longer efficient and companies are moving towards a zero-trust architecture (ZTA). A zero-trust strategy predominantly concentrates on securing data and services but has the potential and necessity to encompass all corporate resources (devices, infrastructure elements, applications, virtual and cloud components) as well as entities (end users, applications, and other non-human agents seeking access to resources) (Scott Rose, 2020). A zero-trust architecture embodies a security paradigm grounded in the principle that organizations must refrain from inherently trusting any entity, whether internal or external to their network boundaries. Instead, they must rigorously verify every connection attempt made by individuals or systems seeking access to the organization's network and resources before authorization.

As per the authors, the primary issue in cyber security management stems from the inability of cyber security management strategies to adapt swiftly to the evolving infrastructure usage demands, given the rapid pace of change in the contemporary landscape. There exists a critical necessity for a more expansive framework as it stands presently. However, numerous authorities in the cybersecurity sector lean towards utilizing and citing solely the trifecta of foundational aspects: confidentiality, integrity, and availability (CIA). Despite this, these elements no longer provide adequate coverage for adeptly administering a company's IT infrastructure guaranteeing security for employees, and establishing trust among partners in the contemporary landscape. As technology complexity advances and societal reliance on it progresses, methodologies must similarly advance. This is especially crucial as technological advancements not only enhance daily living but also foster the rapid development of harmful technologies, resulting in substantial losses for both companies and individuals. Combatting swiftly evolving cyber-attacks and fraudulent methods using outdated methodologies from a decade ago is untenable.

The paper discusses the compliance of the CIA triad model, Parkerian Hexad model, and Boyes model with modern cyber security standards whether the elements included in those models are sufficient to cover the entire industry what are the derivatives or modifications of the aforementioned models, and which of these modifications would be best suited to secure remote working.

The goal of the paper is to supplement the existing models with additional units and adapt the models to the requirements of modern cyber security and business-organized remote work. In this scientific paper, the authors will analyse the modifications of the CIA triad, both in studies by other authors and in various standards.

This paper is organized as follows: Section 2 – Research background – describes the main theoretical features and explains the concept of the CIA triad. Section 3 – Methodology – describes the methodology for existing modifications to the CIA Triad model. Section 4 – Description and theoretical substantiation of the newly obtained model – describes the model developed by the authors, its structure, theoretical basis, and how the model would improve the current situation in the field of cybersecurity from the aspect of remote work. Section 5 – Conclusion – contains the authors' conclusions on the analysis of the CIA triad model and the usefulness and compliance of its available modifications with the requirements of the modern cyber security industry, as well as the conclusions on the new model developed by the authors based on the CIA triad model.

2. Research background

The concept of confidentiality, integrity, and availability, often denoted as the CIA triad serves as a fundamental framework for shaping information security policies within organizational settings. Occasionally, it is alternatively termed the AIC triad (availability, integrity, and confidentiality) to prevent any potential confusion with the acronym associated with the Central Intelligence Agency. While these three pillars constitute vital cybersecurity requisites, there is a consensus among experts that an evolution of the CIA triad is imperative to ensure its continued efficacy (Chai, 2021). The CIA triad is the cornerstone of cybersecurity, and no security policy is thinkable today without it. The Triad consists of three components: confidentiality, integrity, and availability (ISO, 2018).

Considering the rapid development of information technology and the ever-increasing demands for a comprehensive cybersecurity model, the scope should not be limited to the basic elements of cybersecurity, but the scope should be expanded to take into account the latest cybersecurity and technology trends to address current challenges. Many experts in the field are working on such models and many such improvements have been made to the CIA model. The best-known models are the Parkerian Hexad which consists of six elements and the “Boyes model” which consists of eight elements.

Authors have observed a trend that technology and the social environment are increasingly interacting with each other. To solve an issue of a technological nature, it is often necessary to expand the scope and also attract the impact of the social environment to the problem that has arisen. For example, instead of trying to attack a company's infrastructure and

information systems, cybercriminals choose to retrieve information from the company's employees using a variety of social engineering methods.

Almost every day brings news of fresh cybersecurity breaches. In a landscape rife with vulnerable systems and malicious actors, modern organizations find themselves locked in an ongoing struggle to fortify defenses against potential cyber threats, employing both technical and social strategies. Among these, it has been recognized that maintaining a well-informed and vigilant workforce stands out as a particularly cost-efficient method for ensuring organizational resilience in the face of cyber adversaries (Erjon Zoto, 2019), (Khan, 2011). Cyber security issues cannot be solved only by looking from the Information Communication Technologies (ICT) perspective alone. Specialists in both fields, social and technical, are well versed in the nuances of their field, but knowledge and understanding of both sectors are needed to solve today's problems. This requires a more comprehensive examination of how social and technical systems overlap and how this increasing overlap affects cybersecurity.

3. Methodology

With the development of technology and the growing importance of cybersecurity, Parker, the author of the book "Fighting Computer Crime: A New Framework for Protecting Information" (Parker, 1998) presented a six-element system that incorporates all the concepts of the CIA model. The combination of these six elements is called the Parkerian Hexad (Žiga Turk, 2022). To the existing Parkerian Hexad Boyes added resilience and safety to create eight attributes of secure processes (Boyes, 2014), (Žiga Turk, 2022). Tab.1 shows all three CIA (3 elements), Parkerian Hexad (6 elements), and Boyes (8 elements) models.

Table 1: The main elements of cyber security according to the model

	components	CIA Triad	Parkerian Hexad	Boyes Model
1	Confidentiality	X	X	X
2	Integrity	X	X	X
3	Availability	X	X	X
4	Authenticity		X	X
5	Utility		X	X
6	Possession / Control		X	X
7	Safety			X
8	Resilience			X

Explanatory definitions of each model element:

1. Confidentiality – the property that sensitive information is not disclosed to unauthorized entities. Authorized restrictions on information access and disclosure, including means for preserving personal privacy and proprietary information (Elaine Barker, 2019);

2. Integrity – Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity (Elaine Barker, 2019);
3. Availability – Timely, reliable access to information by authorized entities (Elaine Barker, 2019);
4. Authenticity – proof or validity that a claimed identity (whether human or a resource) is real and legitimate (Cybrary, 2022);
5. Utility – Indicates how useful the data is. There can have a variety of degrees of utility, depending on the data and its format (e.g., encrypted or not) (Žiga Turk, 2022);
6. Possession / Control – The methodologies for risk governance, encompassing protocols, methodologies, frameworks, norms, or architectures, may entail administrative, technical, managerial, or juridical dimensions. An attribute allocated to an asset indicative of its comparative significance or indispensability in attaining or facilitating the attainment of predefined objectives (Ron Ross, 2021);
7. Safety – a requirement to ensure that the individuals involved with an organization, including employees, customers, and visitors, are safeguarded from any kind of malicious act or attack (Cybrary, 2022);
8. Resilience – The ability of an information system to continue to operate under adverse conditions or stress, even if in a degraded or debilitated state, while maintaining essential operational capabilities and recovering to an effective operational posture in a time frame consistent with mission needs (Force, 2020).

To understand how to improve or supplement existing models, a definition of the major problems of remote working is needed. The main issue of remote working is:

- phishing scams;
- unsecured endpoint devices;
- home office risks;
- network security.

As we can see from the list of the main problems of remote work, several problems are not exactly related to cyber security risks, but sociological risks. Therefore, to complement this model, it is necessary to look much broader than before, including not only elements related to information security but also elements related to the security of socio-technical systems.

The element of authenticity was already introduced in Parkerian Hexad, which might confuse you, but there are some differences between Authenticity and non-repudiation. Authenticity is about one party (e.g., Alice) interacting with another (e.g., Bob) to convince Bob that some data comes from Alice. Non-repudiation is about Alice showing Bob proof that some data comes from Alice, such that not only Bob is convinced, but Bob also gets the

assurance that he could show the same proof to Charlie, and Charlie would be convinced, too, even if Charlie does not trust Bob.

The disparity between the Parkerian hexad and the Boyes model resides in the incorporation of two additional components, namely resilience and safety. During the formulation of his model, Boyes approached it through the lens of infrastructure management, focusing on the absent elements within the Parkerian hexad that are crucial for ensuring the continuity of services. The Boyes model can be viewed as an expanded version of the Parkerian hexad model, with the inclusion of an aspect dedicated to individual user security and another dedicated to resource operation recovery and resilience. These additions are particularly significant in the context of building management systems and other IT-driven managerial processes. IT systems crucial for continuity and stability are ubiquitous, extending beyond critical infrastructure and building management to a wider user base. Emphasizing end-user security remains paramount in the contemporary landscape.

4. Description and theoretical substantiation of the newly obtained model

Today, information security is associated with the CIA triad, Parkerian Hexad, or the eight-element Boyes model. Working remotely during a pandemic, statistics show that for the most part, the success of the attack was not a technical compromise of systems or resources, but information obtained through social engineering. This is evidenced by the sharp increase in spam and phishing emails. Even if the systems or resources are highly technically secure, there is a very high risk that it may be easily confronted involving people and using social factors against them.

As a result of the research, the authors concluded that it is necessary to create a socio-technical model containing two sub-sections, social and technical. As a result, the following model has been created Fig. 1.

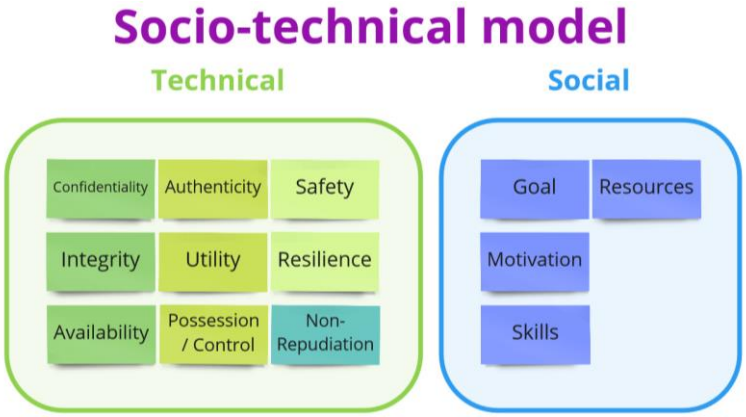

Figure 1: Newly obtained model

4.1 Technical section

The technical section includes all elements of the Boyes model, supplemented by one element of the authors. When working remotely, one of the most important security factors is to make sure that the identity the person is pretending to be is legitimate. Consequently, the authors consider it necessary to supplement the current technical model, which consists of eight elements, with another element called "non-repudiation".

1. Non-repudiation – Ensuring sender authentication and message integrity through cryptographic protocols guarantees evidence of transmission receipt for the sender and verification of the sender's identity for the recipient, thereby precluding subsequent repudiation of information processing by either party (Kevin Stine, 2008). Non-repudiation denotes the irrefutable verification of the veracity of an entity's assertion. This legal concept, ubiquitous in the realm of information security, pertains to a service furnishing evidence regarding data provenance and its unaltered state. Essentially, non-repudiation renders challenging the disavowal of message origin, authenticity, and integrity. Digital signatures, in conjunction with supplementary mechanisms, afford non-repudiation in the domain of online transactions, crucial for preempting repudiation concerning contractual obligation acknowledgment or message dispatch validation. Thus, non-repudiation in this context underscores the imperative that parties involved in a contract or communication embrace the legitimacy of their signature on a document or the transmission of a message.

Although Boyes's eight-element model contains elements that directly refer to non-repudiation, the authors believe that this element needs to be highlighted as a separate element, because remote work and online communication are unthinkable without personal identification and the journaling of identification evidence.

4.2 Social section

To create a set of elements of the social model, the authors included the characteristics of the attacker in the scope defining the attacker's motives, skills, available resources, and desired goals. These social parameters are directly correlated with the technical parameters because based on the attacker's social description, we can determine what kind of the targeted cyberattack will be.

The social subsection includes the following four social elements Fig. 2:

1. **Motivation** – a motivating force, stimulus, or influence;
    a. **Financial gain** – a primary motivation for hackers is the money they can obtain by stealing passwords, and bank details, holding customer information for ransom, or selling data to competitors or on the dark web;

b. **Challenge** – a large portion of hackers are driven by the opportunity to break the unbreakable system and gain recognition from their peers;

c. **Hacktivism** – infamous hacker groups use their skills to target large organizations and embarrass their IT teams, break their sophisticated security systems, and humiliate the upper management;

d. **Revenge** – certain types of hackers are motivated by anger and use their skills to directly affect a person, group, or company without any fear of repercussion;

e. **Subversion** – hackers have been accused of meddling in current and corporate affairs - a modern-day version of espionage;

f. **Infamy** – hackers are motivated by a sense of achievement, working independently or in groups, they want to be recognized.

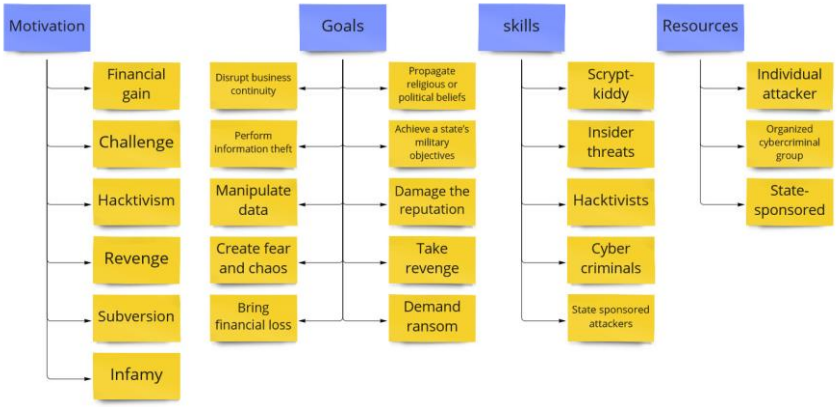

Figure 2: Social section with elements of the newly obtained model

2. **Goal** – the end toward which effort is directed, the desired result of the attack;

   a. disrupt business continuity;

   b. perform information theft;

   c. manipulate data;

   d. create fear and chaos by disrupting critical infrastructures;

   e. bring financial loss to the target;

   f. propagate religious or political beliefs;

   g. achieve a state's military objectives;

   h. damage the reputation of the target;

i. take revenge;

j. demand ransom.

3. **Skills** – the capacity to adeptly apply acquired knowledge in execution or performance. By assessing the proficiencies of the assailant, we can ascertain the potential sophistication of this cyber intrusion;
    a. **Scrypt-kiddy** – the archetype of a script kiddie who employs established, widely recognized methodologies, software, and scripts to identify and capitalize on vulnerabilities within internet-interconnected systems. Their assaults are haphazard and lack comprehensive comprehension of the mechanisms, functionalities, and repercussions of the tools at their disposal;
    b. **Insider threats** – the manifestation of an insider threat poses a significant risk to the security integrity and data sanctity of an organization, originating from sources internal to its operational framework.
    c. **Hacktivists** – hacktivists are individuals or groups of hackers who carry out malicious activity to promote a political agenda, religious belief, or social ideology;
    d. **Cyber criminals** – cybercriminals are individuals or groups of people who use technology to commit cybercrime to steal sensitive company information or personal data and generate profits;
    e. **State-sponsored** attackers – state-sponsored attackers have particular objectives aligned with either the political, commercial, or military interests of their country of origin;
4. **Resources** – a source of supply or support.
    a. an attack by an individual attacker – the available resource options are small;
    b. an attack by an organized cybercriminal group – the number of available resources is relatively higher compared to individual attackers;
    c. a state-sponsored cyberattack – resources are practically limitlessly large.

It is very important to realize that the basic elements of cyber security are not only three, but they are also at least eight and they should not be related only to the technical sphere. These basic elements of cyber security must necessarily contain all the elements proposed by Boyes, as well as binding elements from the social sphere. We cannot rely solely on the CIA Triad elements to successfully manage resources and solutions today. We need to look more broadly at information security.

The socio-technical paradigm represents a holistic strategy merging social and technical elements to effectively comprehend and tackle cybersecurity hurdles. Here are various

rationales supporting the advantageous utilization of the socio-technical paradigm in cybersecurity for countering cyber assaults:

1. **Holistic Comprehension:** Cyber threats frequently originate from a blend of technical susceptibilities and human actions. The socio-technical paradigm aids in grasping the interaction between these facets, offering a more exhaustive perspective of the threat environment.
2. **Human Element:** Individuals often constitute the weakest point in cybersecurity defenses due to factors such as lack of awareness, mistakes, or malicious motives. By incorporating social and organizational aspects, the socio-technical paradigm can target human susceptibilities through training, policies, and fostering a conducive culture.
3. **Risk Oversight:** Efficient cybersecurity revolves around risk management. The socio-technical paradigm assists in pinpointing not only technical vulnerabilities but also the social and organizational contributors to risk. This broader outlook enables enhanced risk evaluation and mitigation tactics.
4. **Resilience:** Cyberattacks are unavoidable, necessitating organizational resilience for enduring and rebounding from such incidents. The socio-technical paradigm underscores constructing resilient systems and teams by amalgamating technical safeguards with human-centered practices like incident response planning and continual enhancement.
5. **Adaptability:** Cyber threats evolve swiftly, rendering static technical solutions prone to obsolescence. The socio-technical paradigm advocates for adaptable and agile cybersecurity methodologies capable of evolving alongside shifting threats and technological landscapes.
6. **Compliance and Governance:** Numerous cybersecurity standards and regulations underscore not only technical protocols but also organizational frameworks and practices. The socio-technical paradigm aligns effectively with compliance requisites by addressing both technical and social dimensions of cybersecurity governance.
7. **Interdisciplinary Collaboration:** Cybersecurity transcends mere IT concerns, presenting a multidisciplinary quandary necessitating collaboration across teams such as IT, legal, HR, and management. The socio-technical paradigm promotes interdisciplinary collaboration by emphasizing the interconnectedness of technical and social systems.

In essence, harnessing the socio-technical paradigm in cybersecurity endeavors can foster more resilient, adaptable, and robust security stances adept at countering evolving cyber threats while effectively addressing human and organizational influences.

4.3 Technical model versus socio-technical model: real-world example

To enhance the comparative analysis of the efficacy between the socio-technical model and technical models like the Boyes model and Parkerian Heksad, this section will juxtapose the influence of the more inclusive Boyes model against the socio-technical model assembled by the authors.

Boyes Model, a comprehensive cybersecurity framework, emphasizes the integration of people, processes, and technology within an organization (Boyes, 2017). It posits that cybersecurity measures must not only focus on technical aspects but also consider human factors and organizational processes. This model recognizes the crucial role of human behavior and organizational culture in cybersecurity resilience. By incorporating elements such as training, awareness programs, and robust policies, Boyes' Model seeks to create a holistic defense strategy against cyber threats.

On the other hand, the Socio-technical Framework emphasizes the interconnectedness of social and technical systems within an organization (Pasquale, 2017). It recognizes that technological systems are embedded within social contexts and that changes in one aspect can impact the other. This framework encourages a multidisciplinary approach, involving collaboration between cybersecurity experts, social scientists, and organizational stakeholders. By understanding the socio-technical dynamics, organizations can design more effective cybersecurity strategies that align with human behaviors and organizational practices.

In a real-world scenario, such as protecting a financial institution against cyber attacks, Boyes' Model would advocate for a comprehensive approach. This would include technical measures such as firewalls, encryption, and intrusion detection systems, along with training programs to educate employees about phishing scams, social engineering tactics, and safe computing practices. Additionally, Boyes' Model would stress the importance of clear policies, incident response plans, and regular security audits to ensure ongoing protection.

On the other hand, the Socio-technical Framework would delve deeper into the organizational culture of the financial institution (Hale, 2020). It would examine how social norms, communication patterns, and decision-making processes influence cybersecurity practices. This framework would recommend interventions such as promoting a security-conscious culture, fostering cross-departmental collaboration on security issues, and conducting socio-technical risk assessments to identify vulnerabilities stemming from human and organizational factors.

In conclusion, while Boyes' Model and the Socio-technical Framework approach cybersecurity from different angles, they are complementary in enhancing an organization's cyber resilience. Integrating both frameworks can lead to a more robust cybersecurity posture by addressing technical vulnerabilities as well as human and organizational behaviors that impact security outcomes.

5. Conclusion

Cybersecurity dilemmas elude resolution solely through computational means. They necessitate a deeper examination of the interplay between social and technical systems, and the consequential impact of this burgeoning convergence on security measures (Sheridan, 2019). The cybersecurity community has a ready understanding of the protocols, services, etc. of a tech platform, but less understanding of how these networks affect society and politics collectively. A burgeoning domain within academia, computational social science delves into the intricate dynamics of societal interactions facilitated by social networks and digital media. However, this realm predominantly overlooks the consideration of these phenomena through the lens of security, much less as a matter pertinent to defense strategies (David Perlman, 2019).

Considering the data elucidated in this paper alongside insights gleaned from the investigation, the researchers posit that addressing forthcoming cybersecurity challenges with greater efficacy necessitates a socio-technical perspective. As a result, the researchers have formulated a socio-technical framework that, in their estimation, may delineate with finer granularity the focal points for new system development and corporate security strategizing.

The future work of the authors will be related to the improvement of this sociotechnical model by studying the security aspects of sociotechnical systems in depth. The authors' future research will be related to the study of socio-technical frameworks that are oriented toward the cybersecurity industry and asset management.

References

Agnes Ekfors Elvin, F. S. (2021). Understanding the Effects of Cyber Security Risks and Threats on Forced Teleworking Organizations. 128. Lund, Sweden: Lund University.

Babulak, E. (2009). Teleworking and Next Generation Cyberpace. *2009 International Conference on Computational Intelligence, Modelling and Simulation*, (pp. 142-146). https://doi.org/10.1109/CSSim.2009.33

Boyes, H. (2014). *Code of Practice for Cyber Security in the Built Environment.* Institution of Engineering and Technology.

Boyes, H. (2017). Cybersecurity for Industrial Control Systems: A New Approach. CRC Press.

Cakula, S. (2022). Secure RemoteWorkplace 4EM Model. In T. A.-H.-S. Faisal Saeed (Ed.), *Advances on Smart and Soft Computing* (pp. 367--377). Singapore: Springer Singapore. https://doi.org/https://doi.org/10.1007/978-981-16-5559-3_30

Chai, W. (2021, January). *confidentiality, integrity, and availability (CIA triad)*. Retrieved 06 20, 2022, from techtarget.com:

https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

Council of the EU. (2022, May 10). *Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union*. Retrieved 06 30, 2022, from European Council - Council of European Union: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

Cybrary. (2022). *Cybersecurity Glossary*. Retrieved 06 22, 2022, from https://www.cybrary.it/resources/glossary/

David Perlman, P. B. (2019). Hacking Ten Million Useful Idiots: Online Propaganda as a Socio-Technical Security Project. *Black Hat USA 2019.* Las Vegas. Retrieved 06 30, 2022, from https://www.blackhat.com/us-19/briefings/schedule/#hacking-ten-million-useful-idiots-online-propaganda-as-a-socio-technical-security-project-15456

Elaine Barker, W. B. (2019). Recommendation for Key Management: Part 2 – Best Practices for Key Management Organizations. *NIST Special Publication*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-57pt2r1

Erjon Zoto, S. K.-R. (2019). Using a socio-technical systems approach to design and support systems thinking in cyber security education. (P. B. S. Kowalski, Ed.) *Complex Systems Informatics and Modeling Quarterly*. https://doi.org/10.7250/csimq.2019-18.04

Force, J. T. (2020, December 10). Security and Privacy Controls for Information Systems and Organizations. *NIST Special Publication 800-53 Rev. 5*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-53r5

Hale, J., & Tokic, D. (2020). *Integrating socio-technical perspectives into cybersecurity risk management. Journal of Cybersecurity*.

ISO. (2018). *ISO/IEC 27001, Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary, International Organization for Standardization*. Retrieved 06 05, 2022, from https://www.iso.org/standard/73906.html

Kevin Stine, R. K. (2008). Information security. *NIST Special Publication, 2*. Retrieved 06 20, 2022, from Computer Security Resource Center: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf

Khan, B. A. (2011). Effectiveness of information security awareness methods based on psychological theories. *African journal of business management, 5*, 10862--10868. https://doi.org/10.5897/AJBM11.067

Limnell, J. A.-B. (2018). *Russian cyber activities in the EU.* European Union Institute for Security Studies (EUISS). Retrieved 06 30, 2022, from http://www.jstor.com/stable/resrep21140.10

Parker, D. B. (1998). *Fighting Computer Crime: A New Framework for Protecting Information. Simon & Schuster.* John Wiley & Sons, Inc.

Pasquale, F. L., & Miskell, J. (2017). *A socio-technical framework for cybersecurity.* Computers & Security, 68, 176-189.

Ron Ross, V. P. (2021, December). Developing Cyber-Resilient Systems: A Systems Security Engineering Approach. *NIST Special Publication 800-160, 2*. https://doi.org/https://doi.org/10.6028/NIST.SP.800-160v2r1

Scott Rose, O. B. (2020). Zero Trust Architecture. *NIST Special Publication*. Retrieved from https://doi.org/10.6028/NIST.SP.800-207

Sheridan, K. (2019, June 24). *A Socio-Technical Approach to Cybersecurity's Problems*. Retrieved June 30, 2022, from darkreading.com: https://www.darkreading.com/perimeter/a-socio-technical-approach-to-cybersecurity-s-problems

Stewart Kowalski, J. M. (2011). Modeling the Enemies of an IT Security Systems - A Socio-Technical System Security Model. Retrieved 06 20, 2022, from https://www.diva-portal.org/smash/get/diva2:469589/FULLTEXT01.pdf

Žiga Turk, B. (. (2022). A systemic framework for addressing cybersecurity in construction. *Automation in Construction, 133*, 103988. https://doi.org/https://doi.org/10.1016/j.autcon.2021.103988