EUROASIA
Matematik, Mühendislik, Doğa ve Tıp Bilimleri Dergisi
Journal of Mathematics, Engineering, Natural & Medical Science

Research Article e-ISSN: 2667-6702 https://doi.org/10.5281/zenodo.15812726

Human Factor Risk Modeling in Cybersecurity: A Scoping Review of KAB Frameworks and Data-Driven Approaches

Aybars BARS [1*], Sabri ERDEM [2]

[1] Dokuz Eylul University, Faculty of Business, Department of Business Administration, İzmir
Corresponding Author Email: aybars.bars@ogr.deu.edu.tr

Article Info

Received: 21.02.2025
Accepted: 25.03.2025

Keywords

Cybersecurity
Decision making
Human factor
Cybersecurity strategy

Abstract: Cybersecurity decision making increasingly demands attention to human factors alongside technical defenses. While frameworks such as ISO/IEC 27001 and NIST guide organizational compliance, the behavioral dimensions of risk perception, bounded rationality, and strategic adaptation remain underrepresented in cybersecurity modeling. This scoping review synthesizes the literature to explore how human factor risk is approached in the context of cybersecurity, with a particular emphasis on Knowledge–Attitude–Behavior (KAB) models and data-driven decision frameworks. Drawing from multiple disciplines, the review identifies patterns and limitations in how cybersecurity decision making processes are conceptualized. The findings highlight a fragmented landscape in which descriptive human behavior insights and normative decision models often operate in isolation. The study concludes by identifying the need for hybrid models that incorporate both behavioral insights and data-driven decision frameworks, offering a promising direction for supporting cybersecurity adaptation in business.

1. Introduction

Cybersecurity is one of the core concerns for organizations across all sectors affecting business continuity, reputation, customer and stakeholder reliability and trust, contracts, and legal issues. While only a decade ago cybersecurity was only a matter of "*If an organization was going to be compromised?*", but today it is a serious concern with the questions of "*What time?*" and "*What level?*" since the threats grow more sophisticated and frequent (Jalali, Siegel, & Madnick, 2019). Technology based countermeasures and defenses are essential but are insufficient on their own.

Decision making in cybersecurity is not only about technical management; it involves complex trade-offs under uncertainty and risk, influenced by governance, regulations and compliance (GRC) requirements, resource constraints, and organizational culture. In real world examples, Chief Information Security Officers (CISOs), information technology (IT) managers, cybersecurity professionals and other decision makers deal with limited information and the bounded rationality to evaluate dynamic risk environments. The integration of human centric models into cybersecurity strategies remains fragmented and needs to be studied further. The human element, considered to be the weakest link in the cybersecurity chain; comprising behaviors, decision making patterns, and risk perceptions, are identified as a critical component of resilience in cybersecurity management.

The Knowledge - Attitude - Behavior (KAB) framework, originally developed in public health and education fields to model individual behavior change. The framework proposes that knowledge influences attitudes, which eventually influences behavior. This model is used in cybersecurity awareness, but its application is limited in decision modeling or supporting the organizational cybersecurity strategy. Additionally, the KAB's linear logic is challenged by findings from behavioral economics and cognitive psychology; since the habits, emotions, contexts, and cognitive biases shape decisions and decision outcomes (Simon, 1957; Brette, Lazaric, & Vieira da Silva, 2017).

This paper presents a scoping review of existing frameworks and models addressing human factor risk modeling in cybersecurity, with particular attention to the KAB based approaches and data driven decision models. By systematically combining insights across game theory, behavioral modeling, decision theory, and agency theory, this review aims to bridge the gap between human centric understanding and quantitative modeling of cybersecurity risk.
The remainder of the paper is organized as follows. Methodology section outlines the methods used in conducting the scoping review, including inclusion criteria and data sources. Findings present four key dimensions: cybersecurity decision making in business contexts; the role of human factors; theoretical and modeling approaches; and the application of KAB frameworks in cybersecurity research. After the discussion of the integration of human-centric and data-driven models, the conclusion section reflects on the implications of the findings and directions for future research. This review builds on the conceptual framework developed during the author's doctoral research.

2. Method

This scoping review draws on a wide range of peer-reviewed studies, frameworks, and theoretical models. Literature is sourced using academic databases (e.g., Scopus, IEEE Xplore, Google Scholar) with search terms such as "human factors cybersecurity," "KAB cybersecurity frameworks," "decision-making under uncertainty," and "cybersecurity modeling." Key inclusion criteria include studies addressing decision-making, simulation, human behavior, and organizational risk in cybersecurity. All the sources are selected based on relevance and citation frequency in high-quality publications.

3. Findings

3.1. Cybersecurity Decision Making in Business

Organizations differ in the view of managing cybersecurity according to their industry and structure, and the Chief Information Security Officer's (CISO) who leads the direction of these efforts as a prominent part of the cybersecurity decision making. There is also a significant difference in decision making between general IT and cybersecurity investment and spending. Compliance considerations, risk appetite, cost-benefit trade-offs, and stakeholder priorities shape the decision outcome (Kissoon, 2020). While the risk appetite is all about how much protection is needed, in case of low-risk perception or tight budget scenarios, "accept risk and do nothing" is also a decision alternative for organizations.

Later, Kissoon (2021) analyzes decisions on implementing specific cybersecurity controls such as multi-factor authentication (MFA), firewall upgrades, and encryption tools. The nature of cybersecurity decisions also includes postponing the cybersecurity investment until the next budget cycle or having sponsorship support from the organization after a breach. Compliance requirements must be satisfied with regulatory or industry standards. Those regulations not only belong to different regions and purposes but also, they are required by different sectors and represent different focuses (Tara Kissoon, 2021). Table 1 below represents an overview of common cybersecurity regulations and frameworks which are an important decision criterion for the decision maker.

Table 1. Common Cybersecurity Regulations and Frameworks (Framework for Improving Critical Infrastructure Cybersecurity, 2018; Tara Kissoon, 2021)

Name	Scope / Region	Focus Area
ISO/IEC 27001	International	Information Security Management Systems (ISMS)
PCI DSS Payment Card Industry Data Security Standard	Global	Security of credit card data
CIS Controls Center for Internet Security Controls	Global	Practical, prioritized cybersecurity best practices
COBIT Control Objectives for Information and Related Technologies	Global	IT governance and management
NIST National Institute of Standards and Technology Frameworks	USA – Widely adopted globally	Risk management, security controls (e.g., SP 800-53, CSF)
GDPR General Data Protection Regulation	European Union	Data protection and privacy; breach notification
CCPA / CPRA California Consumer Privacy Acts	California, USA	Consumer rights over personal data
HIPAA Health Insurance Portability and Accountability Act	USA – Healthcare	Security and privacy of health information (PHI)
GLBA Gramm-Leach-Bliley Act	USA – Financial	Safeguarding consumer financial data
FERPA Family Educational Rights and Privacy Act	USA – Education	Protection of student education records
FISMA Federal Information Security Management Act	USA – Federal agencies	Security requirements for federal information systems

Transferring risks via cyber insurance or outsourcing managed service providers (MSSP) is also a cybersecurity decision alternative. Choosing internal resources and solutions or contracting and outsourcing are also important decision points. The characteristics of cybersecurity products and services cannot be easily compared or replaced with other products while the potential consequences of contract breach can go unnoticed or cause large-scale damages and losses (Nussbaum & Park, 2018). Aside from the nature of information technologies (IT), decisions differ among sectors and one of the causes of this is about contracting schemes.

Nussbaum and Park (2018) identify that cybersecurity decision is though and contracting for cybersecurity has its own unique challenges for government decision making due to concerns in public and social effects. They discuss the common challenges in cybersecurity outsourcing. According to the study, local governments struggle with limited in-house expertise and visibility. Cyber resilience planning is not a trivial task. Their model highlights the importance of risk awareness, and the importance of understanding past incidents in contracting decisions. They also note the hardship in various service definitions, capabilities, and vendor comparisons and due to evolving cybersecurity objectives and lack of standardized benchmarks. The high cost of hardware and software purchases, as well as contracting personnel, which is not easily substitutable, are also concerns. While for the vendor side the learning curve makes it harder, for the buyer side switching vendors is also not feasible in certain circumstances. Table 2 below visualizes the nature of cybersecurity contracting which directly affects the cybersecurity decision making for organizations, some of them have visible consequences and some of them involve unforeseeable risks.

Table 2. Cybersecurity Contracting - Outsourcing Challenges (Johnson, 2015; Kissoon, 2020; Nussbaum & Park, 2018; Vining & Globerman, 1999)

<table>
<tr><td rowspan="6">Hard to Assess</td><td>Cost complexity</td><td>Financial Costs
Investment Costs
Transaction Costs
Bargaining Cost
Opportunity Costs
Governance Costs
Lock-in Costs
Sustainability Costs
Responsibility Costs Service Provision
Reputation / Brand Value / National Defense
Personnel / Intellectual property
other longer-term responsibilities such as Standards / Regulations / Law</td></tr>
<tr><td>Product / Service Complexity</td><td rowspan="4">Nature of cybersecurity products and services are a “post-experience good”. Complex goods are more likely to be affected by unforeseen changes.</td></tr>
<tr><td>Audit/Assurance Testing</td></tr>
<tr><td>Key Performance Indicators</td></tr>
<tr><td>Capacity Maturity Model</td></tr>
<tr><td>Risk of the Attack
(Including False Positives)</td><td>The nature of cyber-attacks in real-world systems that cannot easily distinguish high-risk from low-risk intrusions while requiring real-time monitoring and detection.</td></tr>
</table>

Talent	Cybersecurity Expertise	Specialization of workforce (Education, Training, Certification)
	Specialized local knowledge about physical, terrain, infrastructure, or human geography.	Local knowledge
	Political, Economic, Social, Tech, Law, Environment (PESTLE) Framework	Industry knowledge

Nussbaum and Park (2018) states that allowing cloud-based cybersecurity solutions may combat some of the mentioned challenges previously, explaining the rise in demand for managed cybersecurity services such as Cloud Security Operations Centers (SOC).

3.2. Human factor in cybersecurity

Cybersecurity roles require unique multidisciplinary skills. Bashir et.al. (2017) profiles a cybersecurity talent as having higher self-efficacy and rational decision-making style, and being eager to investigate the phenomena (Bashir, Wee, Memon, & Guo, 2017).

When it comes to technology development, appification promotes information security problems in society. Acar et.al. criticizes the lack of security by design principles as it increasingly allows inexperienced people to develop complex and sensitive apps (Acar et al., 2016) Internet resources such as Stack Overflow are blamed for promoting insecure solutions that are naively copy-pasted by inexperienced developers. At the same time Stack Overflow produced significantly less secure code than those using official Android documentation or books, while participants using the official Android documentation produced significantly less functional code than those using Stack Overflow. Therefore, the authors firmly points out the importance of the need for secure-but-usable documentation (Acar et al., 2016). Not only for application security but also for the cybersecurity industry faces a significant hands on talent shortage (Endicott-Popovsky & Popovsky, 2018).

There are various models and frameworks that focus on the human element of cybersecurity since humans are widely recognized as the weakest link (Jeong, Mihelcic, Oliver, & Rudolph, 2019). In the human domain, it is crucial to understand unsafe actions. Thron and Faily (2022) calls for a holistic view of the human activities, environment and decision-making process for potential cyber security incidents rather than focusing solely only on technology failure or human failure (Thron & Faily, 2022) Main roles of the cybersecurity decision maker include funding the investment cost, implementing the security measures and reviewing the risk appetite statement for the organization (Kissoon, 2020).

The Human Factors Analysis Classification System (HFACS), originally developed as a tool to analyze and reduce human errors in aviation accidents (Shappell & Wiegmann, 2000). HFACS analyzes historical data to find common trends that can identify areas that need to be addressed in an organization in order to reduce the frequency of the errors. The same tool is then proposed with the cybersecurity version to reduce the human error in cybersecurity (Pollock, 2017). Human factors refer to the environmental, organizational and work conditions, to include human and individual characteristics, that influence behavior, which can affect the security of information assets. HFACS is also used by Nobles (2022) to help identify causal

pathways and organizational conditions leading to errors, particularly in cloud computing misconfiguration which is a human error (Nobles, 2022).

A systematic literature review conducted by Rohan et.al. (2021) identifies 17 human factors in cybersecurity. Top five areas are awareness, privacy perception, trust perception, behavior, and capability (Rahman, Rohan, Pal, & Kanthamanon, 2021). Understanding these human factors is essential for improving cybersecurity strategies and anticipating potential issues. However, they criticize research in this area is biased towards Western communities, and more attention should be paid to theoretical research and cultural aspects (Rahman et al., 2021).

A comprehensive trust framework has been developed by Oltramari et.al. (2015). The model moves beyond confidence in technical factors such as hardware, software, infrastructure; it includes trust dynamics which are reserved for humans. Human factors have it own characteristics according to being a defender, user, or even a malicious actor. Figure 1 below shows the actual framework and its variables.

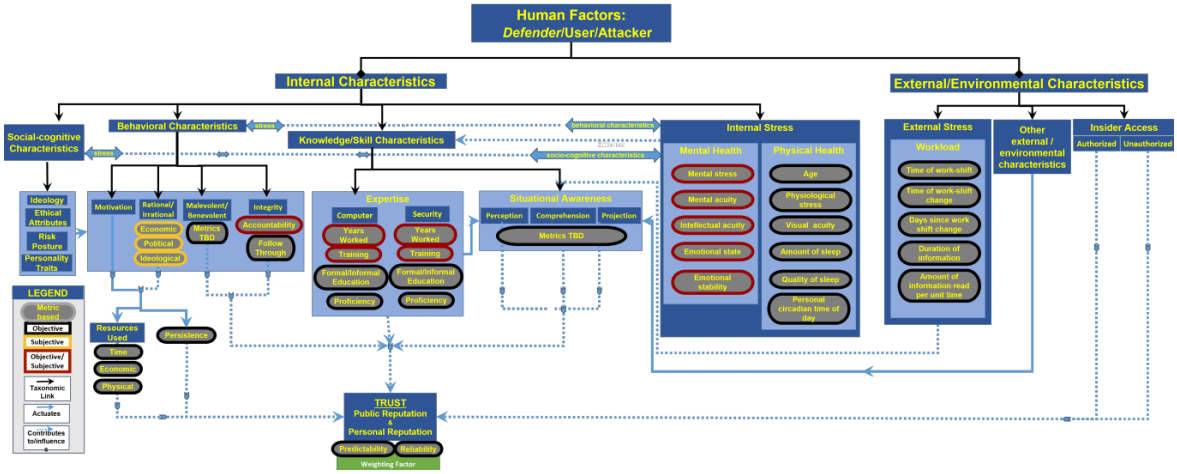

Figure 1. Trust Framework for Human Factor in Cybersecurity (Oltramari, Henshel, Cains, & Hoffman, 2015)

3.3. Theoretical and Modeling Approaches

Dor and Elovici (2016) demonstrates that although organizations have actively implemented cybersecurity frameworks, there is a need to enhance the decision-making process to reduce the number and type of breaches, along with strengthening the cybersecurity framework to facilitate a preventative approach. Studies define possible defenses against cyber-attacks using techniques that can be viewed from three general perspectives, game theory, decision theory and expected utility theory. Agency theory is also leveraged to demonstrate that a decision maker is risk-averse if their wealth portfolio is connected to the organization's performance (Wiseman & Gomez-Mejia, 1998). Game theory, security risk analysis models and event tree analysis is consulted for the cyberattacks and their effects (Kissoon, 2020).

There are studies focus on ways to elicit the knowledge required to understand and model how humans are making cybersecurity decisions with ethical implications too. Researches include human factor as with a unique, complicated mix of personal morality and ethics, along with ideas about what an ethical community, an ethical business, an ethical government, and an ethical society should be (Hoppa, 2018).

Classical real options models typically emphasize staged investment and treat uncertainty as something to be observed and reacted to. However, Benaroch (2018) argues that decision-makers are not merely passive observers; rather, they can proactively shape

uncertainty by implementing early-stage mitigations. This perspective is particularly relevant to cybersecurity, where rapidly evolving threats make passive waiting potentially risky. To adapt cybersecurity in business effectively, decision-makers must act under dynamic threat conditions. These mitigation paths differ in cost, timing, and effectiveness, enabling quantitative trade-offs that enhance cybersecurity investment decisions.

Collier et al. (2013) advocates that cybersecurity decisions should reflect a systems-oriented, risk-based perspective. Their framework categorizes the cyber environment into four interrelated domains: the technical infrastructure, data handling processes, human cognition, and the broader organizational and social context, emphasizing the need for coordinated strategies across these layers. Mentioned four domains are presented at Table 3 below.

Table 3. Four domains of cybersecurity: a risk-based systems approach to cyber decisions (Collier, Linkov, & Lambert, 2013).

Domain Name	Definition
Physical Domain	Hardware, software, and networks as building blocks of cyber infrastructure.
Information Domain	Monitoring, information storage, and visualization
Cognitive Domain	Information should be properly analyzed and sensed as well as used for decision-making in the cognitive domain.
Social Domain	Decisions on cybersecurity should be consistent with social, ethical, and other considerations that are characteristic of their enveloping societal domain.

Dor and Elovici (2016) examine the cybersecurity investment decision-making process in 14 phases represented at the Table 4 below.

Table 4. The Categories and Concepts Emerged from the Grounded Theory (Dor & Elovici, 2016).

Categories (decision process phases)	Concepts
1. External environments of business	A. Strategy
2. Organizational structure or behavior	B. Constraints
3. Understanding of the cyber threat landscape	C. Quality
4. Current information security posture of an organization	D. Prioritization and budgeting
5. Information security gap analysis	E. Applying information security capabilities
6. Identifying the required capabilities	F. Organizational information security education and awareness
7. Identifying relevant alternatives	G. Information security compliance
8. Analysis of alternatives	H. Information security threats
9. Selecting a portfolio of projects	I. Risk management
10. Proof of concept	J. Decision makers
11. Decision and/or execution	K. Decision variables
12. Project initiation	L. Competitive advantage
13. Project planning	M. Doctrine and/or organizational policy
14. Project execution	N. Customer expectations
	O. Implementation
	P. Start-ups

Below conceptual model proposed by Dor and Elovici (2016) shows that the decision-making process is heavily biased by different organizational and psychological factors.

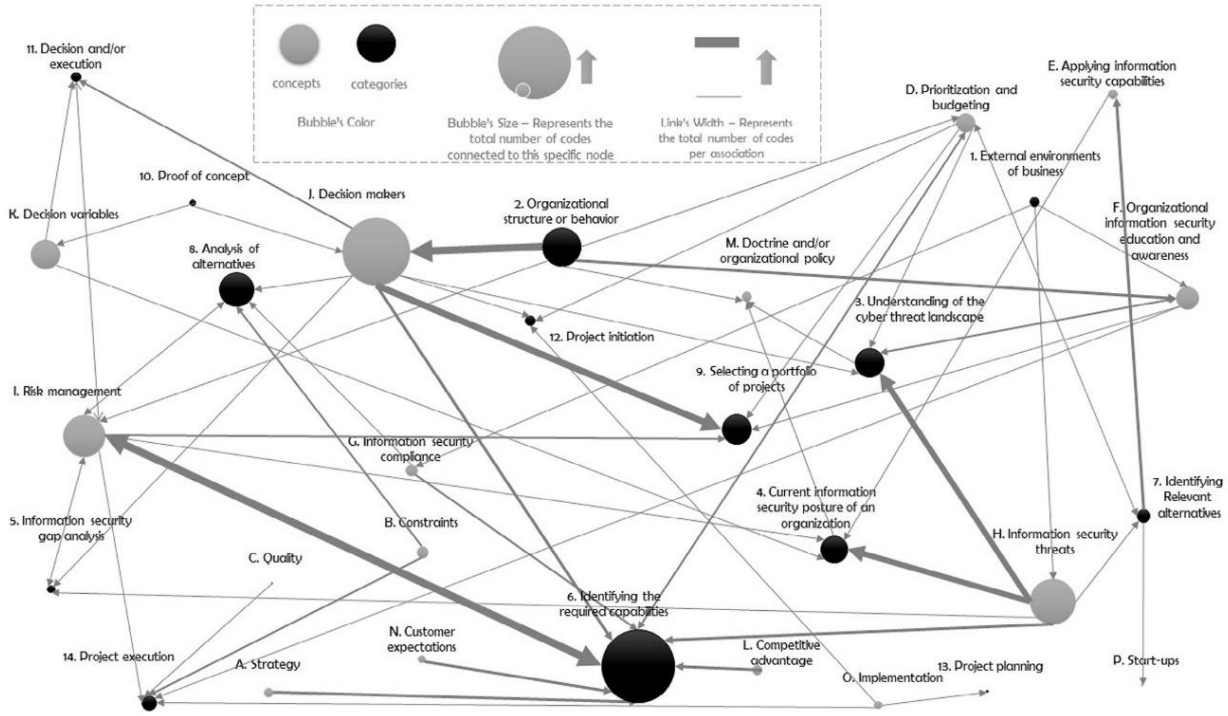

Figure 2. The Conceptual Model of Cybersecurity Decision Making (Dor & Elovici, 2016)

M'manga et.al. (2019) traces the rationale behind cybersecurity decision making during risk and uncertain conditions. Their normative decision-making model illustrates techniques for adapting decision making models to inform system design. The model inspired by Observe – Orient – Decide – Act (OODA) cybersecurity situational awareness methodology. UK Cabinet Office Risk Thinking Model Office proposes a simple iterative process such as identifying risks, assessing risks, building resilience, and evaluating resilience. The risk realization factors given by Figure 3 below are compatible with the findings of Nussbaum and Park (2018) (M'manga et al., 2019).

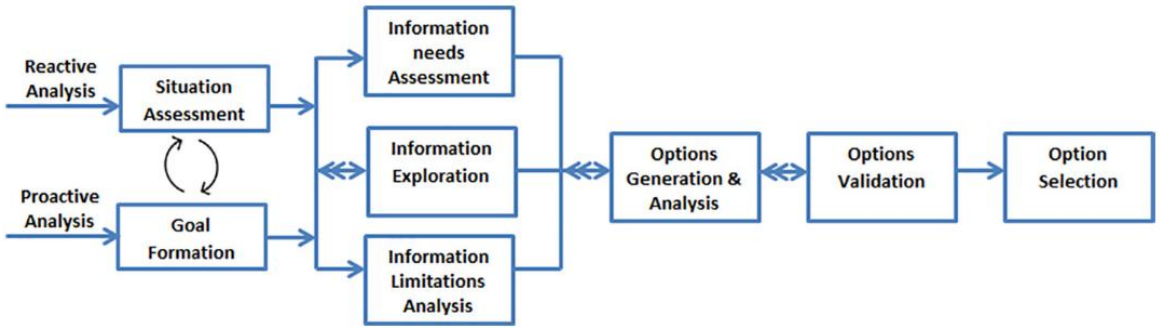

Figure 3. Risk Rationalization Framework (RRF) (M'manga et al., 2019)

Shreeve et.al. (2020) also identify several different patterns of risk based thinking and gain insight into how their decision making process changes as any cyber attacks progress and time passes. Four main mechanisms are used to structure thinking: isolated, sequential, radial, and complex; these describe how a team's discussion and understanding develops. (Shreeve et al., 2020).

While normative approaches model how decisions should be made; descriptive approaches understand how decisions are actually made. Descriptive research on expert decision-making during risk and uncertainty focusses on context-specific decision-making. Normative approaches are usually too high level and generalized, rendering them incapable of providing low-level context-specific guidance (M'manga et al., 2019).

Tiffany et.al. (2017) state that currently, strategy development in cyber is done manually and is a bottleneck in practice even with the usage of some automated tools. They apply game theory toward the augmentation of the human decision-making process (Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, 2017).

Automated techniques and tools for finding, exploiting, and patching vulnerabilities are maturing in cybersecurity but in order to achieve an end goal such as winning a cyber-battle, these techniques and tools must be wielded strategically meaning the irreplaceable element of human factor (Ribeiro, Singh, & Guestrin, 2016).

Different from Tiffany et.al. (2017), Zhang and Liu (2019) states that even existing approaches of cyber-attack-defense analysis based on stochastic game adopt the assumption of complete rationality, but for the actual cyber-attack-defense, it is difficult for both sides of attacker and defender to meet the high requirement of complete rationality. Risk situations bounded by uncertainty as decision alternatives are either unknown or unclear (M'manga, 2020). For this reason, they study the defense decision-making approach based on stochastic games under the restriction of bounded rationality.

Game type	Model assumption	Learning mechanism	Game process	Applicable object	Practicability
Stochastic game	Rationality	—	Multistage	Personal	Bad
Static game	Rationality	—	Single-stage	Personal	Bad
Dynamic game	Rationality	—	Multistage	Personal	Bad
Stochastic game	Rationality	—	Multistage	Personal	Bad
Evolutionary game	Bounded rationality	Biological evolution	—	Group	Good
Stochastic game	Bounded rationality	Reinforcement learning	Multistage	Personal	Good

Figure 4. Comparison of Existing Approaches (Zhang & Liu, 2019)

Zhang and Liu (2019) introduce a cybersecurity decision framework that employs attack–defense graphs to represent threat pathways and corresponding countermeasures. Figure 5 and Figure 6 below depict how these graphs are constructed and applied in their analysis.

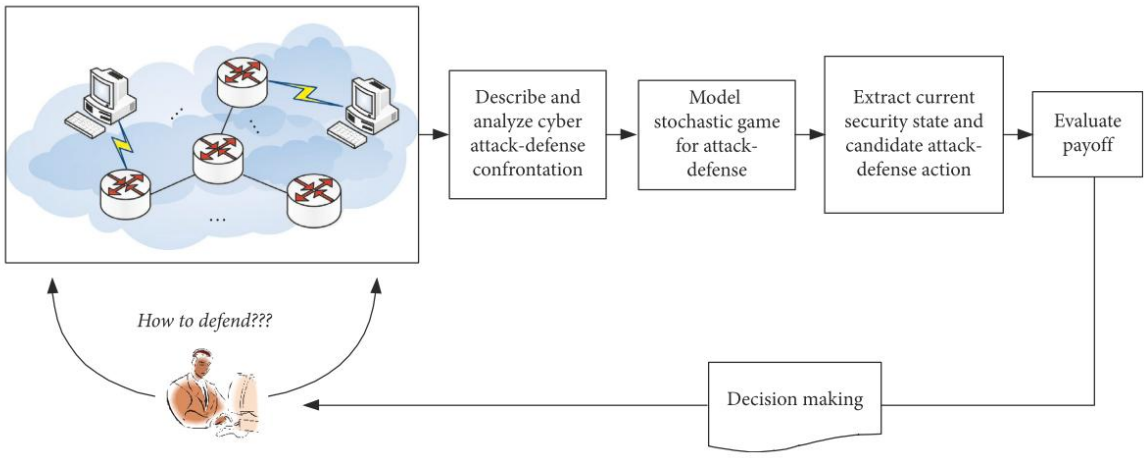

Figure 5. The Process of Cybersecurity Decision Making (Zhang & Liu, 2019)

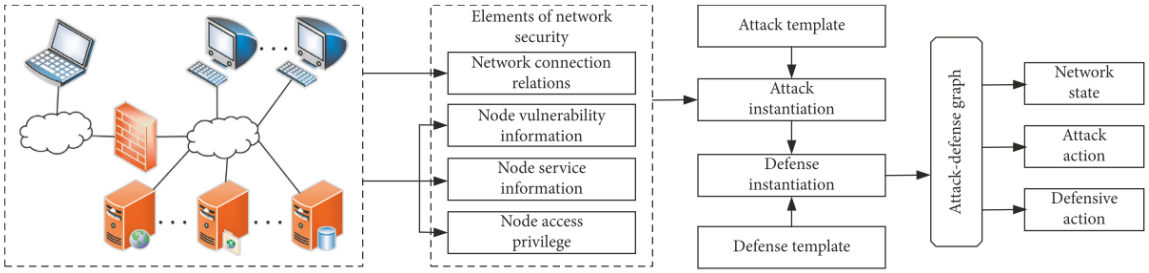

Figure 6. Attack-Defense Graph Generation (Zhang & Liu, 2019)

Jalali et.al. (2019) studies the effectiveness of decision-makers in overcoming two complexities in building cybersecurity capabilities: potential delays in capability development; and uncertainties in predicting cyber incidents. Analyzing 1479 simulation runs, they compare the performances of a group of experienced professionals with those of an inexperienced control group. Both experienced and inexperienced subjects did not understand the mechanisms of delays; however, experienced subjects were better able to learn the need for proactive decision-making through an iterative process. Both groups exhibited similar errors when dealing with the uncertainty of cyber incidents. Their findings highlight the importance of training for decision-makers with a focus on systems thinking skills and lay the groundwork for future research on uncovering mental biases about the complexities of cybersecurity (Jalali et al., 2019).

3.4. The Knowledge-Attitude-Behavior (KAB) Frameworks in Cybersecurity Research

The KAB framework first emerged in 1950s as a practical model in public health, education, and communication. It reflects a linear logic between knowledge, attitude, and behavior and it played a foundational role in applied behavior change initiatives (Launiala, 2009).

Further theoretical models, such as the Theory of Reasoned Action (Fishbein & Ajzen, 2011) and the Theory of Planned Behavior (Ajzen, 1985), consulted on the KAB framework. These frameworks introduced critical constructs like behavioral intention, subjective norms,

and perceived behavioral control, acknowledging that knowledge and attitude alone may be insufficient predictors of behavior.

The KAB frameworks offer a straightforward framework but the assumption of well-informed individuals would make rational choices consistent with their attitudes is challenged by the further research which highlights the role of habit, emotion, social context, and cognitive biases which may shape the behavior (Brette, Lazaric, & Vieira da Silva, 2017; Campitelli & Gobet, 2010; Krämer, 2014; Simon, 1957).

While the KAB frameworks' explanatory depth is challenged, its historical significance and practical utility remain noteworthy (Witte & Allen, 2000). It continues to serve as a baseline structure (Fogg, 2003) in domains like cybersecurity awareness where simplicity and clarity are prioritized over predictive accuracy (Parsons, McCormac, Butavicius, Pattinson, & Jerram, 2014).

4. Discussion

The findings suggest a comprehensive yet fragmented view of theoretical approaches, frameworks, and models in cybersecurity decision making. Since technical studies are significantly more mature compared to human centric dimensions of cybersecurity decision making, decision analysis of humans is underexplored and insufficiently integrated with relevant studies.

Knowledge – Attitude – Behavior (KAB) models offer a beneficial lens for categorizing human risk behavior and understanding individual level security mindset and actions. However, these frameworks are merely integrated into data modeling tools which limit their application in cybersecurity adaptation in business. Human centric models such as HFACS and trust-based frameworks show potential in analyzing the root causes of cyber incidents, their utility in strategic decision making tools remain limited.

Cybersecurity risky behavior and risk appetite may vary in cultural, organizational, and regional variables. However much of the existing literature reflects a Western centric perspective which limits the overall generalizability of scientific research. Variables such as governance, regulations and compliance, public trust, talent capacity and demand, and social norms can significantly influence the effectiveness of both technical controls and human factors in cybersecurity.

Real world complexity includes cognitive biases, bounded rationality, insufficient information, resistance to change, structural rigidities, and resource lock-in. Most of the decision making frameworks do not account for those complexities. Cybersecurity decision makers are often forced to act under pressure, uncertainty, and risk while facing resource constraints, which are highlighted by the models like OODA, risk rationalization frameworks, and observed behavioral patterns in incident response. For this reason, overly rational, prescriptive models may fall short explaining the nature or cybersecurity decision making.

A combination of descriptive behavioral information involving psychology, cognition, judgement, individual and organizational constraints with normative models such as stochastic risk modeling, simulation, and optimization appears to be more promising to help organizations from developing responses to the cyber incidents to develop even more realistic and adaptive cybersecurity strategies.

5. Conclusion

Human factor risk modeling is an under-integrated area in cybersecurity research. This review not only identifies key beneficials of KAB frameworks but also data driven approaches which can better inform organizational decision making. Future work may aim to apply these insights through simulations tools to test and refine decision strategies.

References

Acar, Y., Backes, M., Fahl, S., Kim, D., Mazurek, M. L., & Stransky, C. (2016). You Get Where You're Looking for: The Impact of Information Sources on Code Security. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, 289–305.

Ajzen, I. (1985). From intentions to actions: a theory of planned behavior. *Action Control*, 11–39.

Bashir, M., Wee, C., Memon, N., & Guo, B. (2017). Profiling cybersecurity competition participants: Self-efficacy, decision-making and interests predict effectiveness of competitions as a recruitment tool. *Computers and Security*, *65*, 153–165.

Brette, O., Lazaric, N., & Vieira da Silva, V. (2017). Habit, Decision-Making, and Rationality: Comparing Thorstein Veblen and Early Herbert Simon. *Journal of Economic Issues*, *51*(3), 567–587.

Campitelli, G., & Gobet, F. (2010). Herbert Simon's Decision-Making Approach: Investigation of Cognitive Processes in Experts. *Review of General Psychology*, *14*(4), 354–364.

Collier, Z. A., Linkov, I., & Lambert, J. H. (2013). Four domains of cybersecurity: A risk-based systems approach to cyber decisions. *Environment Systems and Decisions*, *33*(4), 469–470.

Dor, D., & Elovici, Y. (2016). A model of the information security investment decision-making process. *Computers and Security*, *63*, 1–13.

Endicott-Popovsky, B., & Popovsky, V. (2018). Searching and Developing Cybersecurity Talent. *Journal of The Colloquium for Information System Security Education*, (2), 1–17. Retrieved from https://cisse.info/journal/index.php/cisse/article/view/84

Fishbein, M. A., & Ajzen, I. (2011). Belief, attitude, intention and behaviour: An introduction to theory and research. *Reading, Addison-Wesley*, (May 1975).

Fogg, B. J. (2003). *Persuasive Technology: Using Computers to Change What We Think and Do*. Morgan Kaufmann Publishers Inc.

Framework for Improving Critical Infrastructure Cybersecurity. (2018).

Hoppa, M. A. (2018). *Automating Ethical Advice for Cybersecurity Decision-Making*. 170–172.

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cybersecurity capability development: Evidence from a simulation game experiment. *Journal of Strategic Information Systems*, *28*(1), 66–82.

Jeong, J., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *Proceedings - 2019 IEEE 5th International Conference on Collaboration and Internet Computing, CIC 2019*, (December), 338–345.

Johnson, T. A. (2015). *Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare* (1st ed.; T. A. Johnson, Ed.). Retrieved from https://www.amazon.com/Cybersecurity-Protecting-Critical-Infrastructures-Warfare/dp/1482239221.

Kissoon, T. (2020). Optimum spending on cybersecurity measures. *Transforming Government: People, Process and Policy*, *14*(3), 417–431.

Krämer, W. (2014). Kahneman, D. (2011): Thinking, Fast and Slow. *Statistical Papers*, *55*(3), 915–915.

Launiala, A. (2009). How much can a KAP survey tell us about people's knowledge, attitudes and practices? Some observations from medical anthropology research on malaria in pregnancy in Malawi. *Anthropology Matters*, *11*(1), 1–13.

M'manga, A., Faily, S., McAlaney, J., Williams, C., Kadobayashi, Y., & Miyamoto, D. (2019). A normative decision-making model for cyber security. *Information and Computer Security*, *26*(5), 636–646.

M'manga, A. W. (2020). *Designing for Cyber Security Risk-based Decision Making*.

Nobles, C. (2022). Investigating Cloud Computing Misconfiguration Errors using the Human Factors Analysis and Classification System. *Scientific Bulletin*, *27*(1), 59–66.

Nussbaum, B., & Park, S. (2018). A tough decision made easy? Local government decision-making about contracting for cybersecurity. *ACM International Conference Proceeding Series*.

Oltramari, A., Henshel, D., Cains, M., & Hoffman, B. (2015). Towards a human factors ontology for cyber security. *CEUR Workshop Proceedings*, *1523*, 26–33.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers and Security*, *42*, 165–176.

Pollock, T. (2017). *Reducing human error in cyber security using the Human Factors Analysis Classification System (HFACS).* (October). Retrieved from http://digitalcommons.kennesaw.edu/ccerp%0Ahttp://digitalcommons.kennesaw.edu/ccerp/2017/research/2

Rahman, T., Rohan, R., Pal, D., & Kanthamanon, P. (2021). Human Factors in Cybersecurity: A Scoping Review. *ACM International Conference Proceeding Series*.

Ribeiro, M. T., Singh, S., & Guestrin, C. (2016). "Why Should I Trust You?" Explaining the Predictions of Any Classifier. *NAACL-HLT 2016 - 2016 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Proceedings of the Demonstrations Session*, 97–101.

Shappell, S. A., & Wiegmann, D. A. (2000). Office of Aviation Medicine The Human Factors Analysis and Classification System – HFACS. *Embry-Riddle Aeronautical University*, 1–15. Retrieved from https://commons.erau.edu/publication/737.

Shreeve, B., Hallett, J., Edwards, M., Anthonysamy, P., Frey, S., & Rashid, A. (2020). "So if Mr Blue Head here clicks the link⋯" Risk Thinking in Cyber Security Decision Making. *ACM Transactions on Privacy and Security*, *24*(1), 1–29.

Simon, H. A. (1957). Models of Man Social and Rational, Mathematical Essays on Rational Human Behavior in a Social Setting. *John Wiley and Sons, Inc*.

Tara Kissoon, S. (2021). Optimum Spending on Cybersecurity Measures: Part II. *Journal of Information Security*, *12*(01), 137–161.

Thron, E., & Faily, S. (2022). *Automation and Cyber Security Risks on the Railways - the Human Factors implications*.

Tiffany Bao, Yan Shoshitaishvili, Ruoyu Wang, Christopher Kruegel, Giovanni Vigna, D. B. (2017). How Shall We Play a Game? A Game-theoretical Model for Cyber-warfare Games. *IEEE 30th Computer Security Foundations Symposium (CSF)*, 7–21.

Vining, A., & Globerman, S. (1999). A conceptual framework for understanding the outsourcing decision. *European Management Journal*, *17*(6), 645–654.

Wiseman, R. M., & Gomez-Mejia, L. R. (1998). A Behavioral Agency Model of Managerial Risk Taking. *The Academy of Management Review*, *23*(1), 133.

Witte, K., & Allen, M. (2000). A meta-analysis of fear appeals: Implications for effective public health campaigns. *Health Education and Behavior*, *27*(5), 591–615.

Zhang, Y., & Liu, J. (2019). Optimal Decision-Making Approach for Cyber Security Defense Using Game Theory and Intelligent Learning. *Security and Communication Networks*, *2019*.