Revolutionizing Board Cyber-Risk Management Using Collaborative Gaming

Tony Delvecchio[1][a], Sander Zeijlemaker[2][b], Giancarlo De Bernardis[1][c] and Michael Siegel[2][d]
[1]*Cybersecurity Laboratory, BV TECH S.p.A., Milan, 20123, Italy*
[2]*Cyber Security at MIT Sloan, Sloan School of Management, Massachusetts Institute of Technology, U.S.A.*
{tony.delvecchio, giancarlo.debernardis }@bvtech.com
{szeijl, msiegel }@mit.edu

Keywords: Cyber-Risk Management, Security Education, Collaboration, Management Game.

Abstract: International and regulatory developments push cybersecurity into the boardroom. However, strategic group decision-making approach akin to a management board process need to be developed. We used a scientifically grounded cyber-risk management collaborative game in our research. Since not all board members have a solid background in technology and security, we followed the natural user interface design theory to create a management dashboard serious game that fosters an understandable and collaborative setting for managing and educating on cyber-risks. The results show that groups perform significantly better in terms of financial performance and risk profile than individuals. Moreover, the collaborative game allowed executives and business leaders to learn about cyber-risk management issues, thus improving their results. Our future work should focus more on emerging and unpredictable adversarial behavior. Our research has significant implications for security awareness and education in high-level collaborative decision-making bodies.

1 INTRODUCTION

Recent breaches of Atlassian (Kovacs, 2023), MailChimp (Whittaker, 2023), Slack (Burgess, 2023), LastPass (Kapko, 2023), and Dropbox (Gatlan, 2022) show that cyber-risk management goes far beyond compliance. In order to do so, a company must strengthen its strategic decision-making process concerning cyber-risks. Decision-makers tend to have a false perception of security caused by the nature of cybersecurity itself (Zeijlemaker & Siegel, 2023), trust too much in off-the-shelf solutions (Jalali et al., 2019), underestimate both the probability of cyber threats (Jalali et al., 2019) and the impact of cyber threats (De Smidt & Botzen, 2018), and prioritize other business activities (Anderson, 2001).

To strengthen the global state of security, international and regulatory developments push cybersecurity into the boardroom (European Commission, 2022; European Commission, 2020; Pearlson & Hetner, 2022; Zeijlemaker et al., 2022). This implies three critical issues: First, decision-making about cyber-risk management becomes a group process (Bezemer et al., 2014). Second, not all members of this group have a solid background in information technology or cybersecurity (Gale et al., 2022). Finally, this group's strategic dialog focuses on the business, operational, and financial context of cyber-risk. (Pearlson & Hetner, 2022; Zeijlemaker et al., 2022).

Previous research about cyber-risk management did not fully consider these implications because it focused on individual participants (Jalali et al., 2019), with solely technology/security backgrounds (Jalali et al., 2019; Zeijlemaker et al., 2022), or group decisions under stress conditions (Zeijlemaker et al., 2022). These studies did not fully explore the potential benefits of collaboration. Collective intelligence acts differently from individual intelligence because it depends on the collaboration and diversity of the decision-makers' group as shown

[a] https://orcid.org/0009-0004-7940-0521
[b] https://orcid.org/0000-0002-2697-5207
[c] https://orcid.org/0009-0007-6805-4303
[d] https://orcid.org/0000-0002-1483-5530

Delvecchio, T., Zeijlemaker, S., De Bernardis, G. and Siegel, M.
Revolutionizing Board Cyber-Risk Management Using Collaborative Gaming.
DOI: 10.5220/0012349400003648

In *Proceedings of the 10th International Conference on Information Systems Security and Privacy (ICISSP 2024)*, pages 112-119
ISBN: 978-989-758-683-5; ISSN: 2184-4356

in Woolley et al., (2010), Kesari (2021) and Malone (2018) and we believe leveraging on it, can help better managing cyber-risk.

We have included the exercise of Jalali et al. (2019) in a cyber range. Since the human-machine interface has become critically important in strengthening collaboration and decision making (Boy, 2017), we created a user interface that allows for a collaborative and participatory approach to strategic cyber-risk management while explaining cyber-risk management in an accessible and non-technical way. A natural user interface collaborative gesture-based game has been developed and an inverse roulette metaphor has been used for this purpose.

Our research indicates that a collaborative approach to cyber-risk management significantly strengthens organizational performance. The prerequisites for this collaboration are time and space for good dialog before decision-making, as well as providing understandable insights into the matter at hand.

2 LITERATURE

Currently, decisions are increasingly taken through artificial intelligence/machine learning (AI/ML)-enhanced, web-based management dashboards, and decision support (AlSadhan & Park, 2021; Dunie et al., 2015). However, the complex nature of cyber-risk management requires exploration and training in the decision-making process (Jalali et al., 2019; Zeijlemaker et al., 2022; Armenia et al., 2021). This will provide decision makers with an awareness of the topics at hand and an understanding of the consequences of their decision process. It makes the design of user interfaces critical in strengthening decision-makers' understanding and awareness, as well as fostering collaboration in the decision-making process (Wisiecka, 2023).

2.1 Decision Support Tools Usage in Cybersecurity Decision-Making

Cyber-risk management is immensely complex (Zeijlemaker & Siegel, 2023). The risk of security blind spots can overwhelm decision-makers due to complexity and pressure to act. To mitigate this risk, decision-makers use decision-support tools to access and manage cyber-risks (Moore et al., 2016). However, decision-makers are often biased to make decisions that yield immediate, easy-to-observe gains at the cost of long-term, often hard-to-measure consequences (Sterman, 2001).

2.2 The Need for Exploration and Training

Simulation-aided serious games translate system science and simulation modeling into learning experiences (Rooney-Varga et al., 2022; Tseng et al., 2019). They capture human behavior and contribute to knowledge retention, behavioral change, as well as soft skill development.

There is a set of games available that focus on training decision-makers to cope with the complex nature of the cyber-risk landscape (Jalali et al. 2019, Zeijlemaker et al. 2022, Armenia et al. 2021).

All these games recognize the importance of improving decision-making but fail to consider the importance of decision support tool interface design in a collaborative setting with decision-makers who have no ties to technology or cybersecurity.

2.3 Criticality of a Successful Interface Design

In this context, the ability to interact with machines plays a fundamental role in decision making (Jin et al., 2022). A Natural User Interface (NUI) is considered the best way to reduce the communication gap between human and computer, increasing the potential of expert users and making inexperienced users efficient and practical (Wigdor & Wixson, 2011, Fu et al., 2018), especially if it is accompanied by non-verbal communication (Wilson et al., 2008; Bailey et al., 2017; Soro et al,.2011). For this purpose, we use Rapid Iterative Testing and Evaluation (RITE) (Medlock, et al., 2002, 2018) for the design and development of the natural interface and the Mechanics, Dynamics, and Aesthetics (MDA) (Robinet al., 2004; Dwi Putra et al., 2021; Rogério & Frutuoso, 2021; Mohammadzadeh et al., 2022) to refine it.

2.4 Our Contribution to the Literature

Cybersecurity investments are well known to those with adequate training on the subject, but not all members of the group have specific skills in the field, and thus spending money on cybersecurity may be seen as merely a cost by some. The system proposed here consists of a collaborative system with natural interaction that frees the decision-making process from the need to learn how to operate with the system itself. This system guarantees a very rapid learning curve through a simple, automatic, unconscious, and above all, engaging interaction.

3 RESEARCH DESIGN

In the previous section, we explained the criticality of interface design in strengthening collaboration and decision-making. Regarding our research design, we reused a well-appreciated executive training simulation (Jalali et al., 2019) with a new natural user interface to strengthen collaboration in the decision-making process and created a setup to identify this collaboration.

3.1 Explaining the Executive Training Simulation

We used a version of the cybersecurity game by Jalali et al. (2019) that is scientifically grounded in system dynamics and control theory to create a collaborative game for decision-makers with limited knowledge about technology and cybersecurity. This game simulates a strategic decision-making environment for investing in cybersecurity prevention, detection, or response measures. The participant with the highest accumulated profits over the five-year period minimizes the total overall cost for the company and wins the game.

3.2 Design of the Interface and Validation

Using the RITE method, we identified four different metaphors for cybersecurity performance and adopted the "Inverse Roulette" metaphor. The MDA framework was applied to refine the metaphor and present the results with semantic meaning.

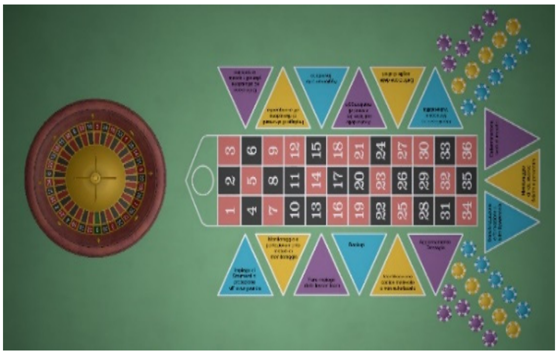

Figure 1: Inverse Roulette.

At the beginning of each simulation step, a hypothetical starting situation is shown on the roulette table, representing the known or unknown vulnerability of the company's ITC systems. The defenders can only bet in suitable areas distributed around the table, representing the cybersecurity defensive measures. By betting on these areas, the users can indirectly operate on the roulette table, switching the transparent yellow (detection) and transparent purple (response) colors to full yellow or full purple colors, or covering other table numbers in blue (prevention).We adopted a performance index to measure the quality of the decision taken. This index is based on the ratio between the accumulated profit and the sum of the systems at risk and the systems affected. Department managers may decide not to enforce strict security policies to reduce costs or realize more profit. However the company's increased risk exposure becomes visible only later in the game.

If the performance index exceeds a pre-defined threshold, it is displayed on the game's roulette board, meaning that budget allocation impeded the attacker from breaching the company's systems.

The performance index/threshold method is suitable for the game, but it lacks meaning from the perspective of learning about cybersecurity. Therefore, another powerful feedback with semantic content is introduced. The final performance index is shown within a 2 x 2 matrix, called Risk-Profit Matrix. It defines a space of four areas in which the final performance index can be plotted: defense gap, risky defense posture, security burden, and balanced behavior.

It is possible to determine what kind of cyber-risk management action should be performed to improve the company's cybersecurity posture considering where the performance index is on this matrix.

In addition to learning about cybersecurity risks and their management, this semantic representation can also serve as a strategic tool for investment planning and cybersecurity posture.

3.3 Research Approach

This study aims to verify whether a collaborative natural interaction game-based system provides learning benefits and better performance. It consists of two phases, both employing the same predetermined attack scenario.

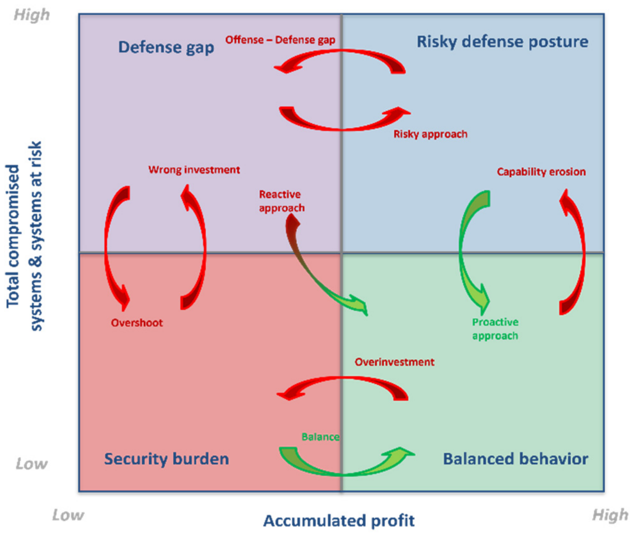

Figure 2: Two-by-two Risk Profit Matrix.

In the first phase, several individual players performed the game a predetermined number of times. In the second phase, a group of users played together for the same number of times. At the end of each session (which involves simulating a time span of five business years), the players are notified of the performance index obtained according to the graphic representation shown in Figure 2. To avoid members of the groups having learned something by playing alone before, those who played as single players cannot play as group members.

The results of single sessions are compared to those of group sessions in order to determine the validity of adopting the collaborative system.

4 RESEARCH RESULTS

We performed ten (3 single players and 7 groups) test sessions using inverse roulette with 100 individuals with different roles and functions, and different skills and experiences. Each session comprises 10 runs, that complete a five-year scenario.

4.1 Performance Index Representation

In each run, a team or a single player allocates investments in cybersecurity measures. The accumulated profit and the number of "affected" and "at-risk" assets at the end of the year are collected. Dividing the former by the sum of the other two, a performance index is obtained. It represents the appropriateness of the allocation choice. Since the scenario is deterministic and is the same for each team and each run, the performance index can be used to compare the performance of the test sessions. The trend of the performance index obtained by each team or single player within their own test session is shown in Figure 3.

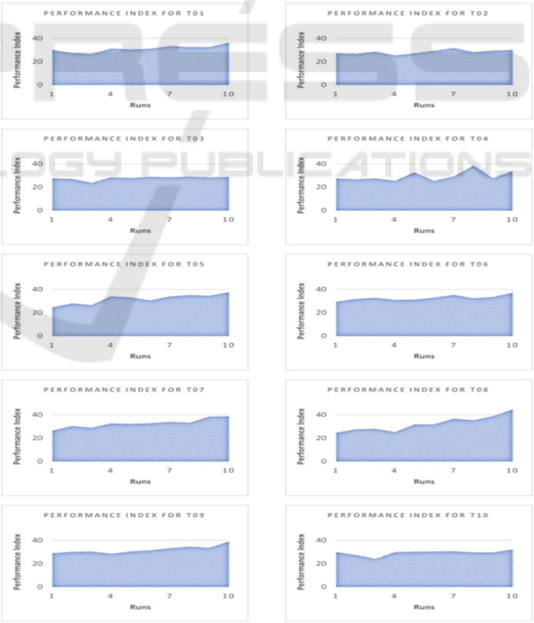

Figure 3: Performance Index obtained in the test sessions.

4.2 Team's Performance Index

Although some performances improve more than others, overall, the trends are positive. This growth is due to two factors: the model is specifically designed to encourage learning about cybersecurity issues, and the natural interface allows users to learn faster. The importance of this second factor is more evident when comparing the results of phase 1 (single-player test session) with those of phase 2 (multiplayer test session).

4.3 Single vs. Multiplayer Performance

There is an observably significant difference in financial performance and risk between single (labeled as T01–T03 in our dataset) and group (labelled as T04–T10) decision-making. We used a t-test (Hair et al., 2006) for comparison. When comparing the total runs of the 10 test sessions combined (8 degrees of freedom), a right-tailed P value of 0.0024 was observed. Additionally, at the level of individual test comparison (98 degrees of freedom), we obtained a significant P value of 0.00000. In both situations, there is a significant difference favoring collective decision-making

Further, regression analysis (Hair et al., 2006) demonstrates the association between performance index and compromised systems and accumulated profit (F = 52 and adj-R2 = 0.51). The regression shows that for every 1-point increase in the performance index, the accumulated profit will increase by 0.01, and for every 1-point increase in the performance index, the compromised systems will decrease by 0.34%. These relationships are very significant as the P value is below 0.001.

Comparing the results achieved for the two types of groups, it is also possible to understand if and how the adoption of a natural interface on a collaborative decision-making system produces notable effects. The results of the groups are superior in terms of performance achieved and in terms of the learning curve, except in two cases. To provide more evidence of the above, a graphic representation is proposed in Figure 4.

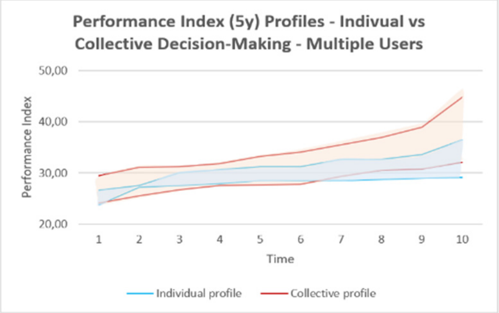

Figure 4: Trend of Performance Index per User Group and Run.

Performance Index in single and group sessions is represented in an aggregated profile view. Only one single player has reached a performance index greater than 35. Another consideration is that the learning curve is faster for teams than for single players, and the performance is higher.

4.4 Risk-Profit Matrix Areas and Learning Path

Another relevant analysis can be performed when all the obtained performance indexes are represented in the Risk-Profit Matrix described in 3.2. These results are shown in Figure 5. Fur purpose of comparison we ran a minimum and maximum baseline scenario. This minimum scenario involves no investments and results in 45% affected assets and 1750 accumulated profits. The maximum scenario involves full investments in all capabilities and yielded 0% affected systems and an accumulated profit of 2275.

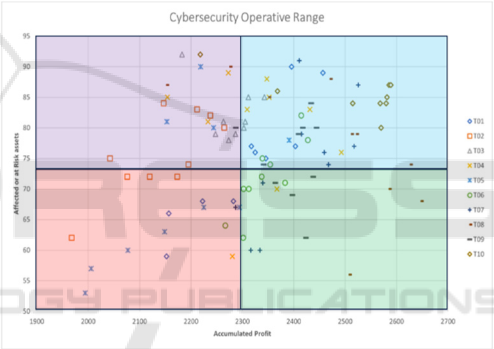

Figure 5: Learning behavior per team across the Risk-Profit Matrix.

Test sessions with better performance index growth tend to "move" toward the Balanced behavior area, where there is a balance between business need and cyber-risk. Each plot can be seen as the “learning path,” that is, how, within the 10 runs, each player/group changes the approach to improve their own performance (see Figure 6). The risky defense posture quadrant appears to play a significant role in learning because it seems that suffering from material threats offers an essential contribution to learning.

The curves represent the learning path each user/group followed to arrive at their last run. The best performances are achieved when the balance behavior area is reached, which has been achieved from T06 and T07 and especially from T09 and T08.

4.5 Discussion and Future Research

This study showed that a cooperative NUI improves cybersecurity budget allocation versus cyber-risk performances in a high-level decision process scenario. Furthermore, it speeds up the learning process and narrows the gap between skilled and unskilled users in strategically managing cyber-risks. The Risk-Profit Matrix graphical representation shows how players change their approach step-by-step within the cybersecurity operative range, from high risk with low profits to high risk with high profits, and ultimately to low risk with high profits. We used different levels of employees to see how such an instrument can be used to improve the learning of the importance of balancing risk versus profits in cyber-security.

The final goal is to propose the game as a powerful tool for raising awareness on the issue of cybersecurity in high-level decision-making contexts in which not all participants are familiar with the specific issue (executives like CEO, CTO, CIO…), allowing roles such as the CISO to make others understand that spending resources on cybersecurity should be seen not only as a cost but as an investment necessary for corporate well-being. However, to better mimic reality, the game can simulate a random attack instead of the deterministic one used in this research. Another significant result could emerge from these scenarios.

5 CONCLUSION

We created a management dashboard serious game with a NUI that fosters an understandable and collaborative setting for managing and educating on cyber-risks. The game allowed executives and business leaders to learn about cyber-risk management issues, thus improving the results of their decision-making process.

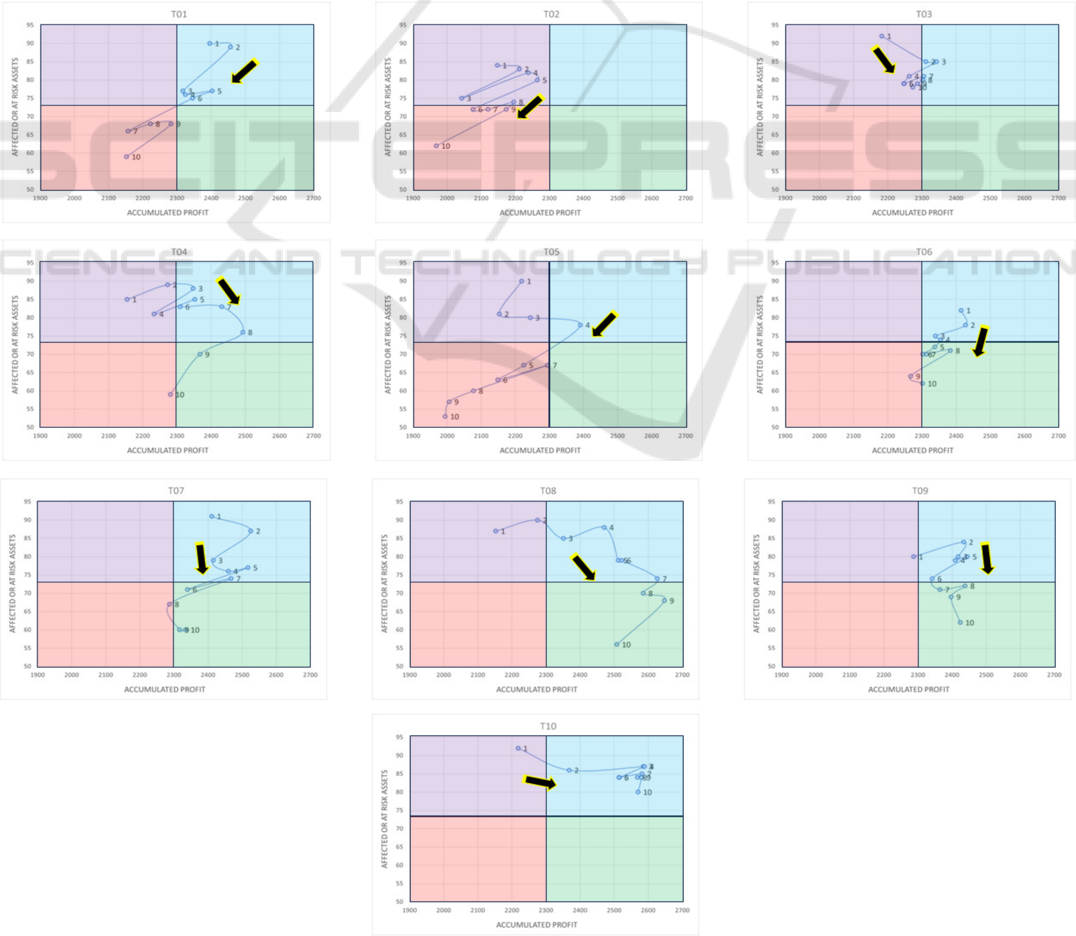

Figure 6: Groups learning paths.

Our work shows that cyber-risk management dashboard design and collaborative board setting are critical drivers for the success of cyber-risk management and is an example of the application of a new kind of collective intelligence where interconnected groups of people and computers doing intelligent things, in our case, manage cyber-risks (Malone & Bernstein, 2022).

ACKNOWLEDGEMENTS

This work was supported in part by the Fondo Europeo di Sviluppo Regionale Puglia Programma Operativo Regionale (POR) Puglia 2014-2020-Axis I-Specific Objective 1a-Action 1.1 (Research and Development) Project Titled: CyberSecurity and Security Operation Center (SOC) Product Suite by BV TECH S.p.A., under grant CUP/CIG B93G18000040007.

REFERENCES

AlSadhan, T., & Park, J. S. (2021, December). Leveraging information security continuous monitoring to enhance cybersecurity. In *IEEE International Conference on Computational Science and Computational Intelligence (CSCI)*, 753–759. doi: 10.1109/CSCI54926.2021.00189

Armenia, S., Angelini, M., Nonino, F., Palombi, G., & Schlitzer, M. F. (2021). A dynamic simulation approach to support the evaluation of cyber-risks and security investments in SMEs. *Decision Support Systems, 147* (113580). https://doi.org/10.1016/j.dss.2021.113580

Anderson, R. (2001). Why information security is hard: An economic perspective. *Proceedings of the 17th annual Computer Security Applications Conference*, 358–365. doi: 10.1109/ACSAC.2001.991552

Bailey, S. K. T., Whitmer, D., Schroeder, B., & Sims, V. K. (2017). Development of gesture-based commands for natural user interfaces*. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 61*(1), 1466–1467.

Bezemer, P. J., Nicholson, G., & Pugliese, A. (2014). Inside the boardroom: Exploring board member interactions. *Qualitative Research in Accounting & Management, 11*(3), 238–259.

Boy, G. A. (2017). *The handbook of human-machine interaction: a human-centered design approach*. CRC Press.

Burgess, M. (2023, January 9*). Security news this week: Don't panic, but Slack's GitHub got hacked.* Wired. https://www.wired.com/story/slack-data-breach-security-news-roundup/

De Smidt, G., & Botzen, W. (2018). Perceptions of corporate cyber-risks and insurance decision-making. *The Geneva Papers on Risk and Insurance-Issues and Practice*, 43, 239–274. https://bit.ly/40lLl4K

Dunie, R., Schulte, W. R., Cantara, M., & Kerremans, M. (2015). *Magic quadrant for intelligent business process management suites*. Gartner Inc. https://iranbizagi.ir/wp-content/uploads/2020/06/Gartner-Reprint.pdf

Dwi Putra, S., & Yasin, V. (2021). MDA framework approach for gamification-based elementary mathematics learning design. *International Journal of Engineering, Science & Information Technology, 1*(3), 35–39. doi: https://doi.org/10.52088/ijesty.v1i2.83

Fu, L. P., Landay, J. A., Nebeling, M., & Zhao, C. (2018, April). *Redefining natural user interface* [Conference presentation]. Extended Abstracts of the 2018 CHI Conference.

Gale, M., Bongiovanni, I., & Slapnicar, S. (2022). Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. *Computers & Security*, 121, 102840.

Gatlan, S. (2022, November 1). *Dropbox discloses breach after hacker stole 130 GitHub repositories*. Bleedingcomputer.com. https://www.bleepingcomputer.com/news/security/dropbox-discloses-breach-after-hacker-stole-130-github-repositories/

Hair, J.H., Black, W.C., Babin, B.J., Anderson, R.E. & Tatham, R.L. (2006). Multivariate Data Analysis, 6th Edition, Pearson, Prentice Hall, Upper Saddle River, New Jersey.

Hee Lee, C. (2020, October). *An inclusive natural user interfaces (NUI) for spatial computing* [Conference presentation]. ACM SIGCHI Mobile. HCI 2020, Oldenburg, Germany. doi: 10.1145/3406324.3410715

Hofmeester, K., & Wixon, D. (2010). *Using metaphors to create a natural user interface for Microsoft Surface* [Conference presentation]. Human Factors in Computing Systems. *Proceedings of the 28th International Conference on Human Factors in Computing Systems* (pp. 4629–4644). Atlanta, GA.

Jalali, M. S., Siegel, M., & Madnick, S. (2019). Decision-making and biases in cyber-security capability development: Evidence from a simulation game experiment. *The Journal of Strategic Information Systems, 28*(1), 66–82. https://doi.org/10.1016/j.jsis.2018.09.003

Jin, Y., Ma, M., & Zhu, Y. (2022). A comparison of natural user interface and graphical user interface for narrative in HMD-based augmented reality. *Multimedia Tools and Applications, 81*(3).

Kapko, M. (2023, March 2). *LastPass breach timeline: How a monthslong cyberattack unraveled.* Cybersecuritydrive.com. https://www.cybersecuritydive.com/news/lastpass-cyberattack-timeline/643958/

Kesari, G. (2021, April, 28). Collective Intelligence Is About To Disrupt Your Strategy: Are You Ready?, April 28, 2021, Forbes. – link: *Collective Intelligence Is About To Disrupt Your Strategy: Are You Ready? (forbes.com)*

Kovacs, E. (2023, February 17). *Atlassian investigating security breach after hackers leak data.* securityweek.com. https://www.securityweek.com/

atlassian-investigating-security-breach-after-hackers-leak-data/.

Malone, T. W. (2018). Superminds: The surprising power of people and computers thinking together. *Little, Brown Spark*.

Malone, T. W., & Bernstein, M. S. (Eds.). (2022). *Handbook of collective intelligence. MIT press*.

Medlock, M. C. (2018). *The rapid Iterative Test and evaluation method (RITE)* (1st ed). OxfordPress.

Medlock, M. C., Wixon, D., Romero, R., & Fulton, B. (2002). *Using the RITE method to improve products: A definition and case* study [Conference presentation]. Usability Professional Association 2002, Orlando, Florida.

McNeill, D. (1992). *Hand and mind: What gestures reveal about thought*. University of Chicago Press.

Mohammadzadeh, Z., Reza Saeidnia, H., Kozak, M., & Ghorbi, A. (2022). MDA framework for FAIR principles. *Studies in Health Technology and Informatics*, 289, 178–179.

Moore, T., Duynes, S., & Chang, F. R. (2016, June 13–14). Identifying how firms manage security investment. *Workshop on the Economics of Information Security (WEIS), Berkeley, California.*

Pearlson, K., & Hetner, C. (2022, November 11). *Is your board prepared for new cybersecurity regulations?* IT Security Management, Harvard Business Review. http://bit.ly/40Jql8v

Rooney-Varga, J. N., Kapmeier, F., Sterman, J. D., Jones, A. P., Putko, M., & Rath, K. (2020). The climate action simulation. *Simulation & Gaming, 51*(2), 114–140. https://doi.org/10.1177/1046878119890643

Robin, H., Leblanc, M., Zubek, R., & Robert. (2004). MDA: A formal approach to game design and game research. *AAAI Workshop—Technical Report, 1*.

Rogério, J., & Frutuoso, G. M. S. (2021). Redefining the MDA framework—The pursuit of a game design ontology. *Information (Switzerland), 12*(10), 395. https://doi.org/10.3390/info12100395

Soro & Alii. (2011). Evaluation of user gestures in multitouch interaction: A case study in pair-programming. *Proceedings of the 13th International Conference on Multimodal Interfaces (ICMI)11*, 161–168.

Sterman, J. D. (2001). System dynamics modeling: Tools for learning in a complex world. *California Manage*. Rev., 43, 8–25.

Tinga, A., Van Zeumeren, I., Christoph, M., & Van Nes, N. (2023). Development and evaluation of a human machine interface to support mode awareness in different automated driving modes. *Transportation Research Part F: Traffic Psychology and Behaviour, 92(1)*, 238–254.

Tinga, A., Cleij, D., Jansen, R. J., & Van Nes, N. (2022). Human machine interface design for continuous support of mode awareness during automated driving: An online simulation. *Transportation Research Part F: Traffic Psychology and Behaviour, 87*(6), 102–119.

Tseng, S. S., Yang, T. Y., & Wang, Y. J. (2019). *Designing a cyber-security board game based on design thinking approach* (pp. 642–650). International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing Advances in Intelligent Systems and Computing (pp. 642–650). Cham, Switzerland.

Tognazzini, B. (2014, March 5). First principles of interaction design (Revised & Expanded). https://asktog.com/atc/principles-of-interaction-design/

Wigdor, D., & Wixson, D. (2011). Brave NUI world: *Designing natural user interfaces for touch and gesture*. Morgan Kaufmann Publishers Inc.

Wilson, A., Izadi, S., Hilliges, O., Garcia-Mendoza, A., & Kirk, D. (2008). Bringing physics to the surface. *Proceedings of UIST*, 67–76.

Wickens. T. D. (2002). *Elementary signal detection theory*. New York: Oxford University Press.

Wisiecka, K., Konishi Y., Krejtz, K., Zolfaghari, M., Kopainsky, B., Krejtz, I., Koike, H., & Fjeld, M. (2023). Supporting complex decision-making: Evidence from an eye tracking study on in-person and remote collaboration. *ACM Transactions on Computer-Human Interaction*. doi:10.1145/3581787

Whittaker, Z. (2023, January 18). *Mailchimp says it was hacked—again.* Techcrunch.com. https://techcrunch.com/2023/01/18/mailchimp-hacked/

Zeijlemaker, S., Etiënne A. J. A. R., Cunico, G., Armenia, S., & Von Kutzschenbach, M. (2022b). Decision-makers' understanding of cyber-security's systemic and dynamic complexity: Insights from a board game for bank managers. *Systems 10*, 2, 49. https://doi.org/10.3390/systems10020049

Zeijlemaker, S. (2022, March 16). *U the dynamic complexity of cyber-security: Towards identifying core systemic structures driving cyber-security investment decision-making*. Radboud University.

Zeijlemaker, S., & Siegel, M. (2023, January 3-6). Capturing the dynamic nature of cyber-risk: Evidence from an explorative case study [Conference session]. *Hawaii International Conference on System Sciences (HICSS)*, Hawaii, 56.