A Simulation-based Education Platform for Security Investments Through Culture and Knowledge Convergence

Adam P. Filippidis[1], Constantinos S. Hilas[1], Anastasios Politis[1], Konstantinos Rantos[2] and Haralambos Mouratidis[3]

[1]Department of Computer, Informatics and Telecommunications Engineering, International Hellenic University, Serres Campus, Serres, Greece

[2]Department of Computer Science, Democritus University of Thrace, Kavala Campus, Greece

[3]Department of Computer and Systems Sciences, Stockholm University, Sweden

adamfilippidis@gmail.com
chilas@ihu.gr
anpol@ihu.gr
krantos@cs.duth.gr
haralambos@dsv.su.se

Abstract: Cybersecurity is one of the most critical sectors of information systems and is considered a strategic priority for many Organizations. Information security investments are a crucial aspect of cybersecurity. However, it often happens that the economic decisions, which aim to improve information security, have poor efficiency. One reason is the lack of background on economics of the Chief Information Security Officers who are often not familiar with the evaluation of the non-technical aspects of security, e.g. economics. The other reason is the cultural gap between the different persons related to business management and administration. In this paper we present an interactive - simulation software designed to familiarize the aforementioned persons with information security investments. The software is actually a game that aims to boost learning for all the stakeholders who are involved in the investment process. A better understanding of the processes, the technical, economic and human factors, along with the cultural convergence of the stakeholders will help boost the efficiency of investments. Design Science is used as the research method. The creative method, a brainstorming technique, is combined with the five steps of Design Science, i.e. explicate the problem, define the requirements, design and develop the artefact, demonstrate the artefact, and evaluate the artefact, to develop a process framework that will be able to cope with this problem. The artefact is an interactive-simulation platform in which a person could take the decision maker role and (a) deal with events that happen and (b) investigate different aspects of information security investment complexity. The evaluation of the artefact is made with a case study in the Industry, where real world data are used to feed the simulation and real-world decision makers play the game in order to better understand the different aspects of the problem and help us trim and enhance the functioning of the platform. Finally, limitations are elaborated and future work is also discussed.

Keywords: Information Security Investments, Game Based Learning, Serious Games, Educational Software, Simulation

1. Introduction

Information security is the practice of protecting an organization's important information and data by mitigating information risks. Information can be physical or electronic, and information security strategies typically encompass a range of measures to safeguard digital data and related assets from cyber threats and attacks, ensuring confidentiality, integrity, and availability of data.

The study of information security investments focuses on understanding and optimizing the allocation of resources to protect information assets from cyber threats. It involves evaluating the effectiveness and return on investment of security measures, identifying critical success factors, and developing strategies to mitigate risks while supporting organizational objectives. The study encompasses various aspects like strategic alignment, economic impact analysis, risk assessment, and the integration of security practices into business processes.

Cybersecurity is a part of information Security and is one of the most critical sectors of information systems since most organizational data are available or can be accessed through the Internet. Thus it is considered a strategic priority for many Organizations. Information security investments are a crucial aspect of cybersecurity. However, it often happens that the economic decisions, which aim to improve information security, have poor efficiency. One reason is the lack of background on economics of the Chief Information Security Officers (CISO) who are often not familiar with the evaluation of the non-technical aspects of security, e.g. economics. The other reason is the cultural gap between the different persons related to business management and administration.

However, despite substantial investments in information security, many organizations find that their economic decisions in this domain often lack efficiency (Schatz & Bashroush, 2017). A key factor contributing to this inefficiency is the lack of economic expertise among CISOs, who traditionally focus on the technical and the

regulatory compliance aspects of security and may not be well-versed in evaluating the economic implications of security investments. Furthermore, a cultural gap often exists between technical security professionals and business management, complicating the alignment of security investments with organizational objectives.

The evaluation of the artefact is conducted through a case study in the industry, utilizing real-world data to validate the simulation and involving actual decision-makers to refine and enhance the platform's functionality. The primary research question guiding this study is: *How can an interactive simulation platform improve the efficiency of information security investments by enhancing the understanding and collaboration among stakeholders?*

The present paper continuous as follows. In Section 2 the background is elaborated. In Section 3 we present the Methodology used for this research, while in Section 4 the artefacts of our approach are presented. Section 5 focuses on the inner workings of the prototype platform. In Section 6 some limitations of this first approach are discussed. Finally, the last Section presents conclusions and makes suggestions for future research.

2. Background

2.1 Importance of Cybersecurity and Information Security Investments

Cybersecurity has emerged as a critical sector within information systems, becoming a strategic priority for many organizations globally. The primary goal of cybersecurity is to protect information by mitigating information risks. This includes preventing unauthorized access, use, disclosure, disruption, modification, inspection, recording, or destruction of information. The increasing prevalence of cyber threats and attacks has highlighted the necessity for robust information security strategies to safeguard digital data and related assets, ensuring the confidentiality, integrity, and availability of information.

2.2 Challenges in Information Security Investments

One of the key aspects of cybersecurity is the investment in information security measures. Nontheless, the economic decisions aimed at improving information security often suffer from poor efficiency. This inefficiency can be attributed to several factors.

CISOs, who are typically focused on the technical aspects of security, may not be well-versed in evaluating the economic implications of security investments. This gap in economic understanding can lead to suboptimal investment decisions that do not fully address the complexities of information security risks. Additionally, the cultural divide between technical and business management teams further complicates the alignment of security investments with organizational objectives.

2.3 Game-Based Learning in Cybersecurity

In order to address the lack of economic expertise of the CISOs and the cultural divide between technical and business management teams, innovative approaches such as game-based learning and serious games have been explored. Game-based learning leverages the engaging and interactive nature of games to facilitate education and training. In the context of cybersecurity, serious games can simulate real-world scenarios, allowing stakeholders to experience and respond to cyber threats in a controlled environment. This method not only enhances learning but also helps in bridging the cultural gap between different teams by providing a common platform for interaction and collaboration (Venter et al., 2019; Williams et al., 2024)

Recent studies have shown that serious games can be an effective tool for teaching complex subjects, including cybersecurity and information security investments. By simulating realistic scenarios, these games enable players to understand the consequences of their decisions and improve their decision-making skills (Williams et al., 2024). Moreover, game-based learning can increase engagement and motivation among learners, leading to better retention of knowledge and skills (Jin et al., 2018e).

For example, a study conducted on the use of game-based learning in cybersecurity education for high school students found significant improvements in both engagement and understanding of cybersecurity concepts (Venter et al., 2019). Another study highlighted the effectiveness of gamification in inspiring and engaging students who are not traditionally inclined towards cybersecurity topics (Williams et al., 2024). These findings are supported by various implementations of game-based learning tools in different educational settings, which

have consistently shown positive outcomes in terms of learning effectiveness and user satisfaction (Tareque et al., 2024; Jin et al., 2018).

2.4 Design Science in Developing Educational Tools

The development of effective educational tools for cybersecurity also involves the application of design science. Design science is a research methodology that focuses on the creation and evaluation of artefacts designed to solve identified problems. This approach is particularly suitable for information systems research, where practical and innovative solutions are needed to address complex challenges (Hevner et al., 2004).

In the context of the current study, design science is used to develop an interactive simulation platform for information security investments. The platform incorporates game-based learning principles and aims to enhance the understanding and efficiency of security investments among various stakeholders. The design process involves iterative cycles of designing, building, and evaluating the platform to ensure it meets the specified requirements (Peffers et al., 2007; Balakrishna & Charlton, 2022).

2.5 Evaluation of Educational Tools

The effectiveness of educational tools like the interactive simulation platform is evaluated through detailed case studies and user feedback. Case studies provide real-world data to validate the simulation, while user feedback helps in refining and enhancing the platform's functionality. The evaluation focuses on several key performance indicators, including user engagement, learning outcomes, decision-making efficiency, and stakeholder collaboration (Balakrishna & Charlton, 2022).

For instance, user engagement can be measured by the time spent on the platform and the frequency of interactions with different simulation scenarios. Learning outcomes can be assessed through pre- and post-interaction assessments to measure improvements in users' understanding of information security investments. Decision-making efficiency can be evaluated by comparing the outcomes of simulated investment decisions with historical data and expert recommendations. Lastly, stakeholder collaboration can be assessed through user feedback and observation of decision-making processes during the simulation (Veneruso et al., 2020).

3. Methodology

Our research adopts the design science approach, a well-established method for creating and evaluating artifacts that solve identified organizational problems. Design science involves iterative cycles of designing, building, and evaluating artifacts until they meet the specified requirements effectively. This methodology is particularly suited for information systems research where practical and innovative solutions are necessary to address complex problems ((Hevner et al., 2004; Peffers et al., 2007).

1. **Explicating the Problem:** The first step in design science is to clearly define and understand the problem. In our case, the problem is the inefficiency of information security investments due to the lack of economic expertise among Chief Information Security Officers (CISOs) and the cultural gap between technical and business management professionals. This step involved a thorough literature review and consultation with industry experts to identify the key challenges and requirements for an effective solution (Peffers et al., 2007).
2. **Defining the Requirements:** Based on the problem analysis, specific requirements for the interactive simulation platform were defined. These requirements included the need for a user-friendly interface, realistic simulation scenarios, and the ability to track and measure the impact of decisions on security investments. The requirements were refined through brainstorming sessions with stakeholders and subject matter experts (vom Brocke et al., 2020).
3. **Design and Development of the Artefact:** The interactive simulation platform was developed using agile software development practices, allowing for iterative improvements based on the feedback from initial users. The platform incorporates game-based learning principles to engage users and enhance learning outcomes. The design process involved creating detailed mockups, developing the software, and conducting initial testing to ensure functionality and usability (vom Brocke et al., 2020).
4. **Demonstration:** The developed platform was demonstrated to a food industry company with 15 million Euro revenue and a workforce of 350 employees over full production periods, and included the CISO, business managers, and other stakeholders. This demonstration aimed to showcase the platform’s capabilities and gather initial feedback on its effectiveness and user experience. The demonstration

also included simulated scenarios where users could make decisions related to information security investments and observe the outcomes (Hevner et al., 2004).

5. **Evaluation:** The final step in the design science approach is the evaluation of the artifact. This was conducted through a detailed case study in the food industry, where real-world data was used to validate the simulation. The evaluation involved actual decision-makers using the platform to simulate information security investment scenarios. The effectiveness of the platform was assessed based on user feedback, the accuracy of the simulation outcomes, and improvements in the understanding and collaboration among stakeholders (Jin et al., 2018 ; Fischer-Hübner et al., 2021).

3.1 Data Collection Methods

Data collection for this study included both qualitative and quantitative approaches:

1. **Interviews and Brainstorming Sessions:** Interviews with industry experts and brainstorming sessions with stakeholders were conducted to gather insights into the challenges of information security investments and to define the requirements for the simulation platform (Hevner et al., 2004).
2. **Case Study:** A case study approach was employed to evaluate the platform in a real-world setting. Data was collected from the participating organization, including historical security investment data, decision-making processes, and feedback from users who interacted with the platform (Hevner et al., 2004). Our Case study was the aforementioned food industry company located in northern Greece.
3. **Surveys and Questionnaires:** Surveys and questionnaires were distributed to users after they interacted with the simulation platform. These instruments were designed to collect feedback on the usability, effectiveness, and educational value of the platform (Hevner et al., 2004), in order to improve the artefacts.

3.2 Evaluation and Analysis

The evaluation of the simulation platform focused on its ability to improve decision-making efficiency and stakeholder collaboration. Key performance indicators (KPIs) were used to measure the platform's impact, including:

1. **User Engagement:** The level of user engagement was assessed based on the time spent on the platform and the frequency of interactions with different simulation scenarios (Williams, Anthi, Cherdantseva, & Javed).
2. **Learning Outcomes:** Improvements in users' understanding of information security investments were measured through pre- and post-interaction assessments.
3. **Stakeholder Collaboration:** The platform's impact on fostering collaboration between technical and business stakeholders was assessed through user feedback and observation of decision-making processes during the simulation (Fischer-Hübner et al., 2021).

The analysis involved both descriptive and inferential statistics to determine the effectiveness of the simulation platform. Qualitative data from interviews and surveys were analyzed using thematic analysis to identify common themes and insights.

4. Artefact Presentation

In this section we present three artefacts. A cybersecurity capability heatmap used for assessing maturity in the organization, some specially crafted key performance indicators (KPIs) to indicate the current preparedness status of the company, and a digital platform used to examine different investment scenarios.

4.1 Maturity Heatmap Artefact

Table 1 is a cybersecurity maturity to technological measurement deployment capability heatmap. The table shows, at a given moment, the cybersecurity maturity of the organization in the three core elements, People, Processes and Technology. For example, people may have the abilities that are demanded for a given measurement, but the technologies used in the organization could be too old. In this case a new investment or a new process is needed to efficiently cope with the specific aspect. To make this simple, imagine the lack of a deployed anti-malware solution in the company, where we must purchase one, or, even worse, the case of an existing anti-malware solution that is not correctly deployed because processes are missing.

Table 1: An instance of the cybersecurity capability heatmap used in the platform

Maturity / Measures		Technology	Process	People
Initial	Physical Security	1	1	1
	Asset Inventory	1	1	1
	Device Hardering	1	1	1
	Patch Management	1	1	1
	Access Controls	1	1	1
Managed	Unidirectional Gateway	2	1	2
	IDS/IPS	1	2	2
	Anti-Malware	2	1	1
	Firewall	1	2	3
Defined	Zone Firewalls	1	1	1
	Device Firewalls	1	2	1
	Whitelisting	2	1	2
Quantitatively Managed	SIEM	2	2	3
	Incident Management	2	2	4
Optimizing	Threat Intelligence	3	3	3

Maturity levels have the following meaning:

Level 1: Basic capability in the organization. Success depends solely on individual non-repeatable non scalable efforts. High risk still exists as effort is inconsistent and attacks unpredictable.

Level 2: Some basic processes are defined, established and documented which makes it possible to have repeatable efforts with goals and measurements.

Level 3: Documentation, standard implementation, maintenance, learning and training are gaining focus which reflects in advanced capabilities.

Level 4: Data collection and monitoring is semi-automated and human capability expertise is proven by acting proactively. Metrics are tracked and not just implemented.

Level 5: Constantly improving through feedback from processes**,** people capabilities are expert, cutting edge technology is implemented. Security is automated, integrated and predictive.

4.2 Key Performance Indicators on Investments Artefact

Key Performance Indicators (KPI's) help to convert raw data to information that provides the user with a quick understanding of security investment decisions. Below we present some KPI's specific for security investments.

Table 2: KPIs of information security investments.

KPI Name	Calculation	Explanation
Maturity ratio Ability of knowledge acquisition	Is the sum of all heatmap Current capability levels for the organization divided to total levels for the three categories.	The heatmap ideal level for each implementation is five, but each organization has a different target level and goals that is driven by asset-to-protect value.
Acceptable Risk Exposure KPI	An Economic value GOAL set by management as acceptable cost in self-assessment minus current cost divided by current incident costs.	A value close to zero or negative means that incidents are more that the accepting risk one. Such a value is an indicator of investment need.
Human capability ratio	It's the total achieved score for people capabilities in the heatmap divided by the sum of total score for human capability for this number of measures (see table 1).	It shows the ability of people to support the current and new investments. A value close to zero means little maturity for the organization and people need training. Comparing with organization maturity or solution needed maturity the expert can identify need for improvement.

KPI Name	Calculation	Explanation
Technology capability ratio.	Its the total achieved score for technology capabilities in the heatmap divided by the sum of total score for technology capability for this number of measures (see table 1).	It shows the ability of the technology implemented to support processes and security needs. A value close to zero means little maturity for the organization. Comparing with organization maturity or solution needed maturity the expert can identify need for improvement.
Process maturity ratio.	Its the total achieved score for process capabilities in the heatmap divided by the sum of total score for process capability for this number of measures (see table 1).	It shows how processes add value (above maturity level of the organization) or create risk for security effort. Comparing with organization maturity or solution needed maturity the expert can identify need for improvement.
Cybersecurity Risk Asset Ratio (CRAR)	It the acceptable cost for security minus current assets at risk divided to acceptable cost for security.	When a risk takes the High flag in the risk register an estimation of asset at risk is made. CRAR is calculated to show the organizational exposure to risk. This should not be higher from the acceptable risk. A value below 0 means that if total assets at risk exploit simultaneously, the cost could be higher from acceptable cost.

5. A Prototype Platform for Security Investments

In this Section the inner workings of the prototype platform, which have been designed in order to help cybersecurity practitioners and managers to assess security risks and related investments are presented.

In Figure 1 the structure and the logic of the platform is depicted. As can be seen in the diagram, a self-assessment procedure is needed in order to generate the company's cybersecurity capability heatmap. Another prerequisite is that the organization's cybersecurity staff should assess, evaluate or even guess the probable risk of malicious or destructive events happening, and file the values in the appropriate Risk Register. Finally, the cost of any security related problems that either happened or may happen, e.g. infrastructure failure or data breaches, should be elaborated and added to an appropriate input screen (table). These costs include the cost of labour to solve the problem, the cost of any equipment and/or software procured to replace any damaged one and of course the cost of the losses due to the incident, e.g. loss of data, reputation, stock value, etc. All these are used as inputs to estimate and generate the Key Performance Indicators which are then used to provide clues for decisions on whether an investment on security is needed along with the size and the type of the investment. Should my company invest on hiring or training personnel? Should we invest on technology procurements, whether hardware of software solutions? Or shall we invest on elaborating the existing (on not existing) procedures within the organization?

The platform presented in Figure 1 is a game where the Security Officer of the company can compete with other decision makers. By competing in this game players will create an understanding of different aspects of security investments (technical and economic), and by trying to self-assess and improve processes, people skills and technology, the stakeholders will create a common culture through knowledge convergence. KPIs thresholds were selected by stakeholders of the case study company and the Security Officer. The development of the game took many iterations with feedback brainstorming sessions in order to be able to satisfy both technical and managerial stakeholders.

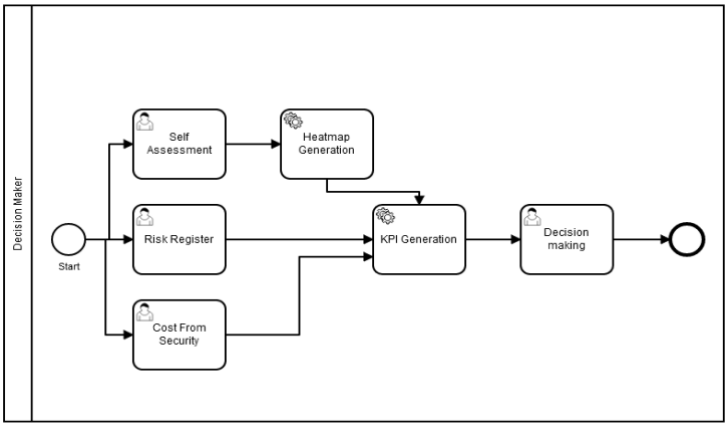


Figure 1: Diagram of the platform's logic and structure

The capability matrix presented in Table 1 is generated by the self-assessment and is a screen where the user can choose to add/edit/delete measurements. The user can add a new measurement and the system dynamically adjusts the corresponding values and automatically presents the updated self-assessment. Figure 2 shows the self-assessment screen.

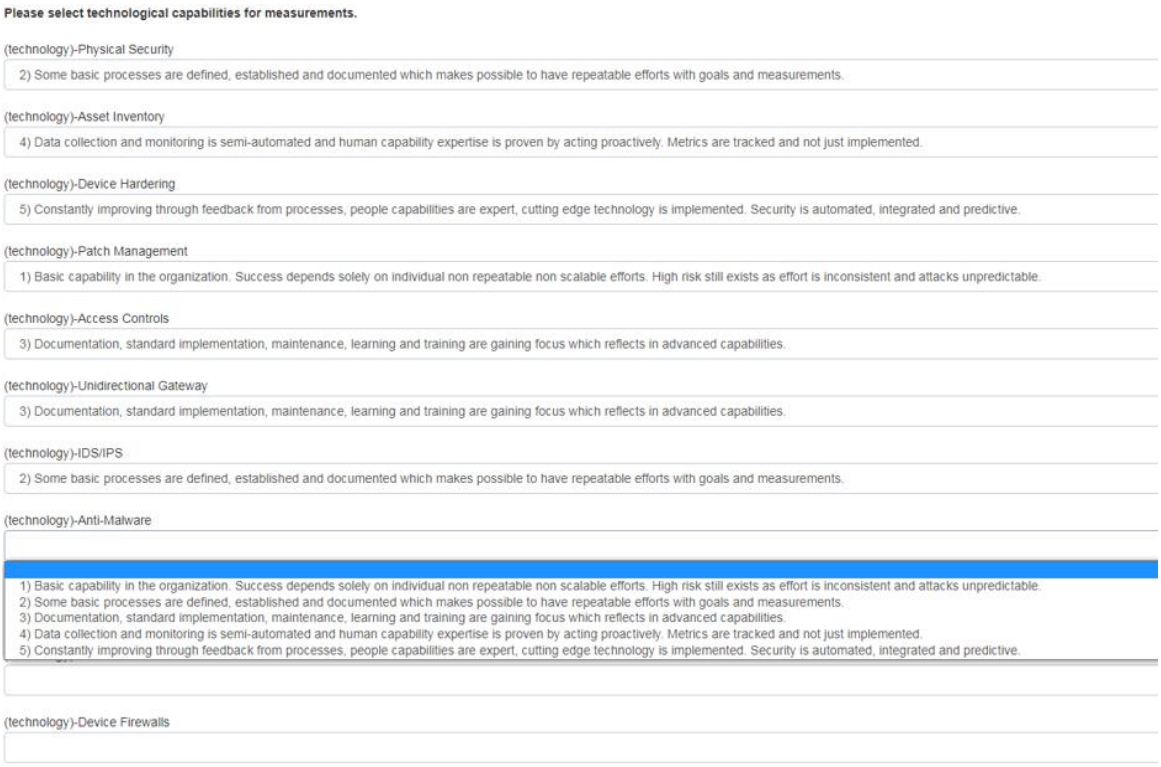
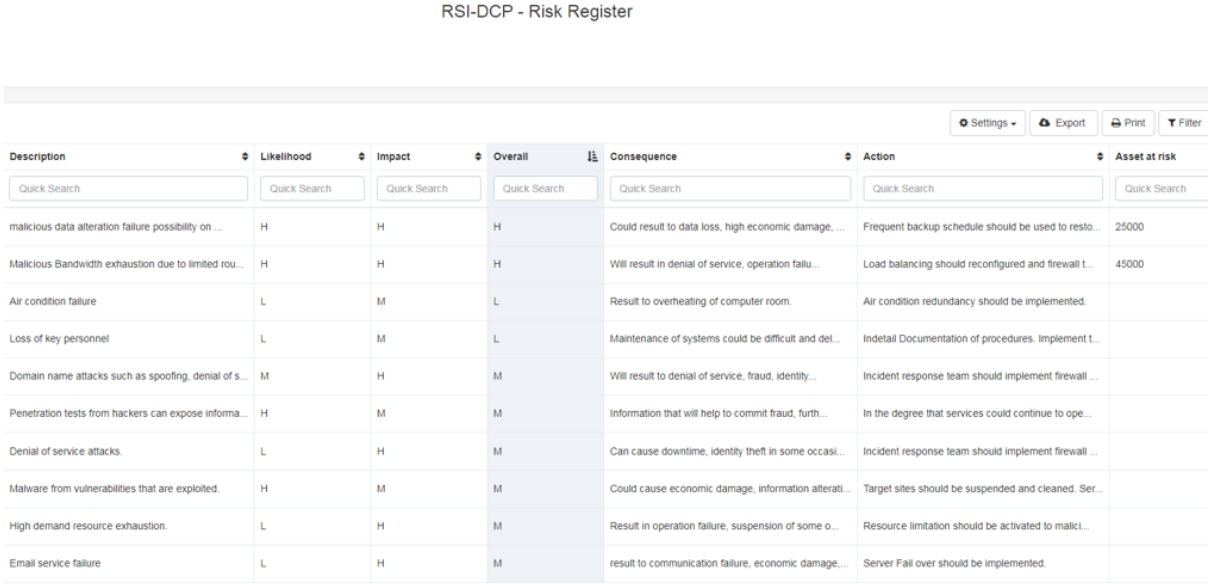


Figure 2: Self-assessment screen

The Risk Register contains all the information about threats for the company. If a threat is changed to a High score, then the decision maker has to put an asset at an estimated risk value. This is an estimateof the possible cost if the asset is exploited. Data from a former real incident may also be used here. The user can add/edit/delete and filter threats. Also, the user can add new threats and set threat name, Likelihood, Impact, Overall score, Consequence if exploited, and action if exploited. Figure 3 show the Risk Register screen.



Description	Likelihood	Impact	Overall	Consequence	Action	Asset at risk
Quick Search	Quick Search	Quick Search	Quick Search	Quick Search	Quick Search	Quick Search
malicious data alteration failure possibility on ...	H	H	H	Could result to data loss, high economic damage, ...	Frequent backup schedule should be used to resto...	25000
Malicious Bandwidth exhaustion due to limited rou...	H	H	H	Will result in denial of service, operation failu...	Load balancing should reconfigured and firewall t...	45000
Air condition failure	L	M	L	Result to overheating of computer room.	Air condition redundancy should be implemented.	
Loss of key personnel	L	M	L	Maintenance of systems could be difficult and del...	Indetail Documentation of procedures. Implement t...	
Domain name attacks such as spoofing, denial of s...	M	H	M	Will result to denial of service, fraud, identity...	Incident response team should implement firewall ...	
Penetration tests from hackers can expose informa...	H	M	M	Information that will help to commit fraud, furth...	In the degree that services could continue to ope...	
Denial of service attacks.	L	H	M	Can cause downtime, identity theft in some occasi...	Incident response team should implement firewall ...	
Malware from vulnerabilities that are exploited.	H	M	M	Could cause economic damage, information alterati...	Target sites should be suspended and cleaned. Ser...	
High demand resource exhaustion.	L	H	M	Result in operation failure, suspension of some o...	Resource limitation should be activated to malici...	
Email service failure	L	H	M	result to communication failure, economic damage,...	Server Fail over should be implemented.	

Figure 3: Risk Register Screen

In the Cost of Events screen (Figure 4) the user can add a new security breach event that had a financial impact to the company. The user can add/edit/delete events. The events have a date, an IT labour cost, the cost of products that bought in order to fix the breach, and the financial loss due to breach. Also, the user can automatically see the total cost graph of all the events until now.

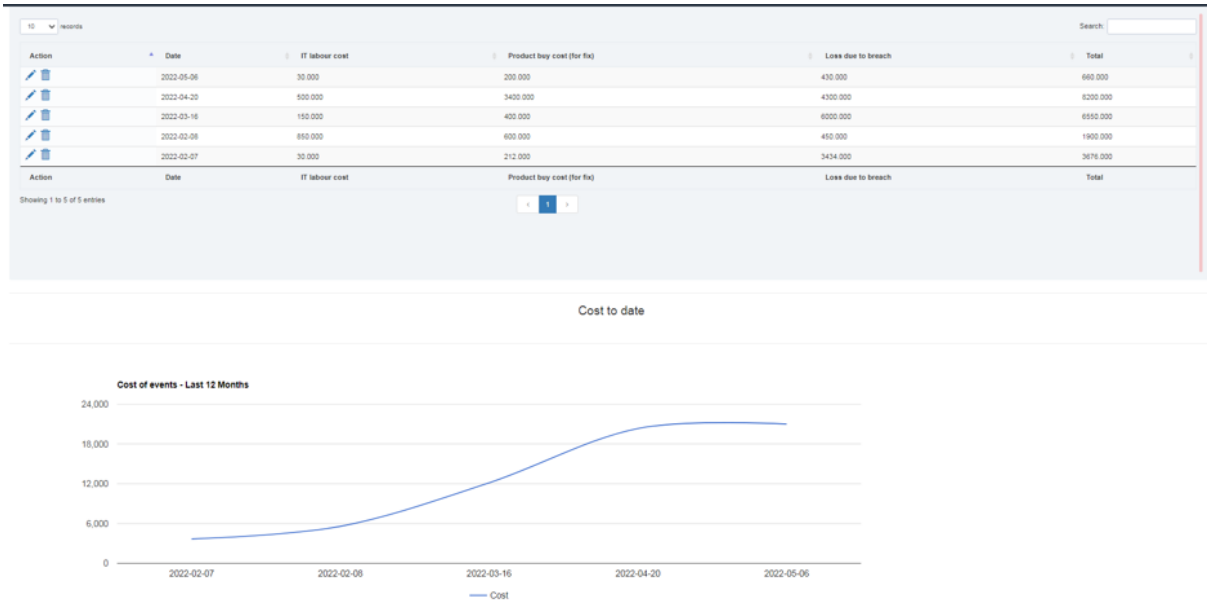


Figure 4: Cost of Events screen

The Calculated KPI screen (Figure 5) shows the automated calculations of the KPIs based on the self-assessment, the risk register and the Incident costs. The user can see the KPI name, the description that explains how the KPI works and what it means, the current KPI value and status. If the KPI status is “AT RISK” it means that some action is required such as a security investment.

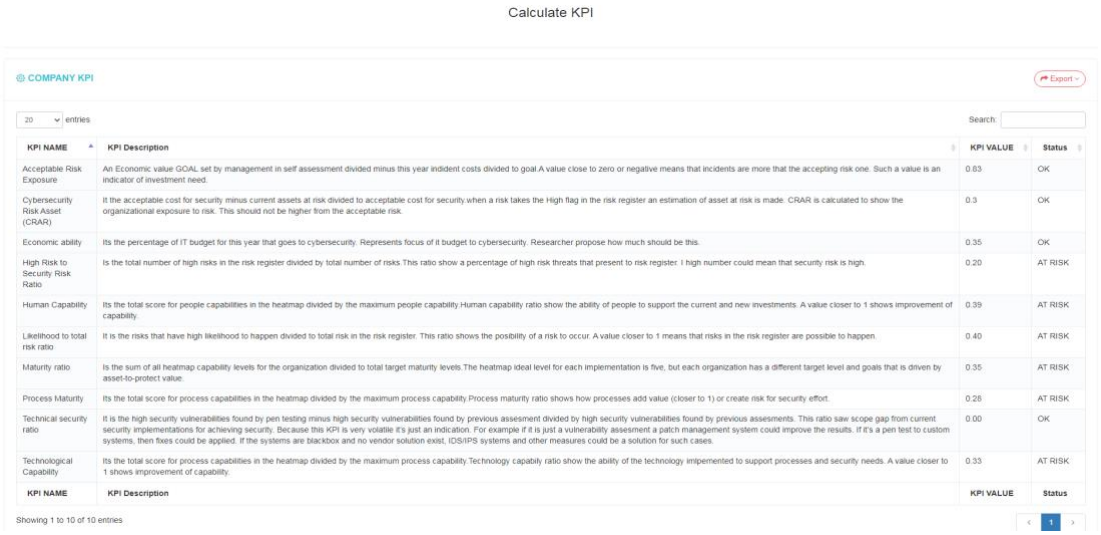


Figure 5: Calculated KPI screen

6. Limitations of our Approach

This research tries to improve the problem of IS investment efficiency by educating CISOs and business managers on risk assessment and optimum security investments. However, limitations apply. First of all, the findings from the case study come from a single industry and may not be applicable to other companies with different characteristics and challenges. Next, while useful for educational purposes, the simulation game may not fully capture the complexities and unpredictability of real-world information security investment decisions. The effectiveness of the simulation relies heavily on the accuracy and relevance of the real-world data used to feed

the platform, so the design and development could introduce biases based on the assumptions and perspectives of the developers. The evaluation of a single case study might not be sufficient to thoroughly assess the effectiveness and efficiency of the simulation platform. Finally, the study may not provide sufficient evidence on the long-term impact of the simulation-based learning on the actual decision-making and investment efficiency because of the limited time used. Our future research will try to alleviate, handle or eliminate these limitations.

7. Conclusions and Discussion

The development of an interactive simulation platform for information security investments addresses significant challenges faced by organizations in aligning technical and economic aspects of cybersecurity. This platform leverages game-based learning principles to bridge the knowledge gap between Chief Information Security Officers (CISOs) and business managers, fostering a collaborative environment where stakeholders can enhance their understanding of investment impacts. By simulating real-world scenarios, the platform enables users to make informed decisions, by promoting efficient allocation of resources to mitigate cyber threats. The design science methodology underpins the development process, ensuring that the platform is iteratively refined based on user feedback and real-world data.

The evaluation through a case study demonstrates the platform's potential to improve decision-making efficiency and stakeholder collaboration. Users' engagement, learning outcomes, and decision-making efficiency are key performance indicators that validate the platform's effectiveness.

To enhance the generalization of the findings, future research could involve conducting case studies across a variety of industries. This would help to identify industry-specific challenges and adaptations needed for the simulation platform, providing a more comprehensive understanding of how different sectors can benefit from such educational tools. Conducting more deployments to assess the long-term impact of the simulation platform on decision-making and investment efficiency is essential. Also, future work should focus on developing customizable modules within the simulation platform to address the unique needs of different organizations. By embedding knowledge, data and feedback from a specific company into the platform will make it capable to cope with scenarios specific to this company. The influence of non-economic factors, such as regulatory compliance, ethical considerations, and psychological impacts, on information security investments should also be explored. Finally, incorporating advanced gamification techniques, such as adaptive learning paths, personalized feedback, and competitive elements, could enhance user engagement and learning outcomes.

In conclusion, this interactive simulation platform aids cybersecurity education, providing a practical tool to improve information security investment efficiency through enhanced stakeholder collaboration and understanding.

References

Balakrishna, C., & Charlton, P. Using Game-based Learning Methods to Demystify Cyber Security Concepts for Adult Learners. *Proceedings of the European Conference on Games-based Learning, (2022), 73-80, 2022-October*.

Fischer-Hübner, S., Alcaraz, C., Ferreira, A., Fernandez-Gago, C., Lopez, J., Markatos, E., . . . Akil, M. Stakeholder perspectives and requirements on cybersecurity in Europe. *Journal of Information Security and Applications, (2021), 102916, 61*.

Hevner, A. R., March, S. T., Park, J., & Ram, S. Design science in information systems research. *MIS Quarterly: Management Information Systems, (2004), 75-105, 28(1)*.

Jin, G., Tu, M., Kim, T.-H., Heffron, J., & White, J. Evaluation of Game-Based Learning in Cybersecurity Education for High School Students. *Journal of Education and Learning (EduLearn), (2018), 150-158, 12(1)*.

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems, (2007), 45-77, 24(3)*.

Schatz, D., & Bashroush, R. (2017). Economic valuation for information security investment: a systematic literature review. *Information Systems Frontiers, 19(5). https://doi.org/10.1007/s10796-016-9648-8*.

Tareque, H. M., Deutekom, S., Anvik, J., & Bashir, M. You Hacked My Program! Teaching Cybersecurity using Game-based Learning. *The 26th Western Canadian Conference on Computing Education, (2024), 1-7*.

Veneruso, S. V., Ferro, L. S., Marrella, A., Mecella, M., & Catarci, T. A game-based learning experience for improving cybersecurity awareness. *Italian Conference on Cybersecurity, (2020)*.

Venter, I. M., Blignaut, R. J., Renaud, K., & Venter, M. A. (2019). Cyber security education is as essential as “the three R’s.” . *Heliyon, 5(12). https://doi.org/10.1016/J.HELIYON.2019.E02855*.

vom Brocke, J., Hevner, A., & Maedche, A. (2020). Introduction to Design Science Research. Στο J. vom Brocke, A. Hevner, & A. Maedche, *Design Science Research. Cases.* Springer.

Williams, L., Anthi, E., Cherdantseva, Y., & Javed, A. Leveraging Gamification and Game-based Learning in Cybersecurity Education. *Journal of The Colloquium for Information Systems Security Education, (2024), 8, 11(1)*.