Journal homepage: https://itce.vn.ua/en

Information Technologies and Computer Engineering **Vol. 23, No. 1. 2026**

Article's History: Received: 14.11.2025 Revised: 16.02.2026
Accepted: 26.03.2026 Published: 20.04.2026

ISSN 1999-9941; e-ISSN 2078-6387
UDC 004.056.5
DOI: 10.31649/vitce/1.2026.35

Interactive visualisation and analysis of risks with a human factor

Viktoriia Trofymchuk*
Master, Lecturer
State University "Kyiv Aviation Institute"
03058, 1 Liubomyr Huzar Ave., Kyiv, Ukraine
https://orcid.org/0000-0002-9756-0244

Abstract. The human factor remains one of the key vulnerabilities in modern cybersecurity, which emphasises the importance of analysing user behaviour in risk management systems. This study presents a comprehensive mathematical model for personalised risk assessment of digital user behaviour, followed by interactive visualisation to support operational decision-making. The aim of the research was to create a model that allows for accurate analysis of individual and situational vulnerability factors, prediction of risky behaviour, and adaptation of protective measures in real time. For the model implementation, a combination of Bayesian analysis, Markov decision-making processes, regression methods, and modern data visualisation tools was used. As a simulation-based, the model was tested on 500 artificially generated user profiles reflecting different levels of digital literacy and behavioural responses to phishing scenarios. The results showed that individualised training significantly reduces the risk of phishing attacks – in some cases by 40%. The built model achieved a prediction accuracy of 85%, demonstrating high efficiency even when taking into account behavioural exceptions. It was found that stress, time constraints, and difficult conditions increase the probability of errors by 25%. At the same time, regular interaction with simulated threats makes it possible to build stable skills – the so-called "risk memory" – which reduces the number of errors over time. The model integrated both behavioural parameters – level of knowledge, stress tolerance, user experience – and external factors, including the threat complexity and workload intensity. This allows for dynamic adjustment of security strategies. Use of Markov modelling allowed optimising training processes, reducing losses by 65%. Interactive dashboards provided individualised vulnerability monitoring and rapid response to potential threats. The practical value of the proposed approach lies in the possibility of its integration into corporate security systems and use in educational and telemedia programmes to improve cybersecurity

Keywords: mathematical modelling; data visualisation; Bayesian analysis; Markov processes; social engineering

Introduction

Cybersecurity is one of the key areas of information protection in the modern digital world. The number of attacks on information systems keeps growing, and the level of threats requires constant improvement of methods to prevent and stop these attacks. One of the main weaknesses is still the human factor – the social, psychological, and behavioural traits of users that directly affect security. According to the ENISA (European Union Agency for Cybersecurity) (2024), more than 70% of cybersecurity incidents happened because of user mistakes or social engineering attacks in 2024. The report also says that these types of incidents grew by 38% compared to 2022. The Verizon Business (2024) Data Breach Investigations Report gave similar results and confirms that human-related risks remain the main cause of security breaches.

Modern security systems, like cryptography, intrusion detection systems, and multifactor authentication, help reduce risks, but these technologies cannot totally get rid of the human factor. H. Ahmad *et al*. (2024) investigated the effectiveness of multi-layered security systems and found that even with strong technical barriers in place, social engineering remains the primary cause of most successful attacks. The authors emphasise that raising user awareness and training in safe behaviour

Suggested Citation:
Trofymchuk, V. (2026). Interactive visualisation and analysis of risks with a human factor. *Information Technologies and Computer Engineering*, 23(1), 35-45. doi: 10.31649/vitce/1.2026.35

*Corresponding author

have a long-term effect that exceeds the benefits of purely technical solutions.

Y. Qin *et al*. (2025) analysed the effectiveness of user training policies for preventing social engineering attacks under resource constraints. The authors showed that the optimal distribution of training interventions can increase user resistance to manipulation and significantly reduce the likelihood of successful compromise without increasing costs. The study also confirmed that even minimal adaptation of training policies can shape more stable user behaviour patterns, which in the long run reduces the risk of social engineering attacks.

The study by A. Alshehri (2024) explored AI-powered adaptive cybersecurity awareness training in the industrial sector. The author showed that using intelligent algorithms to personalise the training process increases the effectiveness of forming stable, secure user behaviour and reduces the response time to potential incidents. The study emphasises that adaptive learning based on artificial intelligence is an effective tool for strengthening the human factor in cyber defence and for systematically reducing risks associated with social engineering attacks. N. Sugunaraj (2024) created a hybrid model that combines regression analysis and machine learning methods to continuously update user risk profiles. The results showed a reduction in errors by almost 30% and the model's resistance to changes in input data, making it suitable for long-term use in corporate monitoring systems.

The use of Bayes-oriented structures makes it possible to obtain more realistic risk assessments compared to classical static analysis schemes. J. Wang *et al*. (2020) proposed a Bayesian approach to cyber risk assessment by extending the FAIR model and formalising the relationships between technical parameters and user behavioural factors. The authors showed that such a network allows for more accurate assessment of uncertainty and formal probabilistic conclusions with limited or incomplete input data. The study confirmed that.

Finally, K. Ahmed *et al*. (2024) proposed a deep learning-based method for the joint extraction of cyber entities and relations from unstructured cybersecurity text. This approach demonstrates that automated information extraction can support cyber threat analysis by organising heterogeneous security data into structured representations. The authors indicate that such methods enhance the analytical capabilities of cyber defence systems and facilitate more effective threat modelling in complex and evolving digital environments.

Even though cybersecurity research is growing rapidly, some problems remain. Most models still do not mix personal user traits – like knowledge, experience, and ability to handle stress – with outside factors such as how hard the attacks are, how much work people have, or changing conditions. Systems that can train users in real time and adjust protection strategies are not well-developed. Also, interactive visuals and dashboards are usually used only to watch what is happening, not to help predict and manage risks directly. The goal of this study was to create an integrated mathematical model for personalised cyber risk assessment. The model took into account both user behaviour and external factors, adapted training and protection strategies in real time, and used interactive visualisation to support decision-making.

Materials and Methods

The study involved simulation modelling of user behavioural responses to phishing attacks using generalised profiles. Parameterised scenarios were created in the Python environment using the SimPy framework for event-based modelling and the NumPy and pandas libraries for generating user attributes and interaction rules. A total of 500 hypothetical users (aged 18-60) were generated with different levels of digital literacy, stress resistance, and previous experience in countering cyber threats. The approach to formalising the mathematical model was based on previous experience in constructing optimisation models in related studies by the author (Trofymchuk, 2025). These scenarios replicated typical behavioural patterns described in leading scientific studies on phishing response (Ahmad *et al*., 2024) and allowed the evaluation of the proposed mathematical model under various levels of risk exposure. The modelling considered user reactions to different types of phishing attacks, including mass phishing e-mails, spear phishing with personalised messages, and social engineering through fake technical support requests. The methodology for evaluating the impact of these attacks on behavioural parameters was based on the approach proposed by M. Zaoui *et al*. (2024).

Statistical analysis of the simulation outputs was performed in the Python environment using the scipy.stats package. The analysis followed standard reliability criteria: p-values with a significance threshold $\alpha = 0.05$ and 95% confidence intervals were calculated to verify differences between groups. Regression analysis and the least squares method were used to calibrate model parameters by minimising the difference between predicted and simulated risk values and by estimating the impact of each factor – user awareness, attack complexity, and environmental conditions – on the overall probability of a successful attack.

The optimisation of training strategies was implemented using the Value Iteration algorithm (via the mdptoolbox library), which identified the sequence of awareness training and defensive actions that minimised the total expected loss $J(\pi)$ and determined the time points when introducing protective measures would yield the highest effect. Model sensitivity to key parameters was examined using a one-factor-at-a-time (OFAT) approach combined with Monte Carlo simulations (10,000 random samples per run). This allowed testing how changes in awareness, attack complexity, or environmental stress affected the calculated risk and adapting the risk management framework to different operational profiles of an organisation.

The development of a mathematical model for assessing cyber risks associated with the human factor was a key

element of the study. User awareness (U) was defined as the simulated level of cybersecurity knowledge and training, attack complexity (A) described the technical and psychological sophistication of phishing attempts, and environmental impact (E) represented stress conditions such as workload, time pressure, and policy support. The schematic representation of the proposed mathematical model of a successful security breach P is presented in Figure 1.

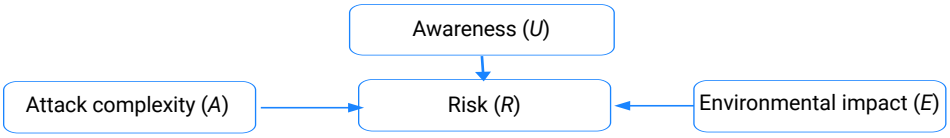

Figure 1. Diagrammatic representation of the mathematical model
Source: compiled by the author

It shows the relationship between the key variables – user awareness (U), attack complexity (A), and environmental impact (E) – and the resulting probability of a successful security breach (P). To ensure interpretability and reproducibility of the model, the parameters require a clearly defined scale and explanation of how the numerical values are set. This step makes it possible to link the visual structure of the model with the following mathematical formulation and to justify the ranges of α, β, γ, δ and other coefficients used in the equations:

$$P = f(U, A, E) = \alpha \cdot e^{-\beta U} + \gamma \cdot \delta \cdot E. \quad (1)$$

Parameters γ and δ represent sensitivity to external contextual variables such as stress or fatigue and were tuned based on behavioural deviations introduced into simulation environments. The term "behavioural exceptions" in this context refers to unpredictable deviations from typical user behaviour patterns – for instance, a digitally literate (Anderson, 2020) user failing to recognise a phishing threat due to psychological fatigue. These exceptions were incorporated into the model by adjusting either α or δ, allowing the model to remain adaptive in unstable behavioural conditions. All parameter values were validated using simulation-generated datasets and calibrated through iterative modelling of hypothetical user-phishing interactions reflecting real-world scenarios.

The proposed user risk assessment model is based on an exponential decrease in risk due to the level of awareness, but unlike classical models, it takes into account the influence of the environment and cognitive factors through the variable E. Additionally, the parameter σ is introduced, which allows flexible adjustment of the model for different attack scenarios, which increases the accuracy of risk prediction.

$$P = \alpha \cdot e^{-\beta U} + \gamma \cdot \delta \cdot E + \rho \ ln(1 + I_t), \quad (2)$$

where I_t – is the intensity of attacks in period t (the number of hacking attempts, phishing emails, social attacks, etc.); ρ is the coefficient of user sensitivity to attacks (determines how much an increase in attacks increases the likelihood of compromise). If a user receives a lot of phishing attacks, even with high awareness U, the user may eventually make a mistake. The logarithmic relationship $ln(1 + I_t)$ reflects the effect of the accumulating pressure of attacks – at first, the risk increases rapidly, but gradually stabilises. The value of I_t can be obtained by normalising the number of recorded incidents in security monitoring systems (e.g., SIEM logs) (NIST, 2020) over a specific time window. This allows the model to dynamically reflect variations in the threat landscape and to adapt to sudden spikes in attack intensity. The parameter ρ characterises the user's reactivity to increasing attack pressure. The model supports adaptive calibration of this parameter based on user characteristics such as digital literacy, stress resilience, or previous exposure to cyber threats. For instance, users with limited technical skills or high susceptibility to stress may be assigned higher values of ρ to reflect increased vulnerability. In simulation scenarios, ρ ranges between 0.05 and 0.2, representing different behavioural response profiles.

Consideration of user experience:

$$P = \alpha \cdot \beta (U + X) + \gamma \cdot \delta \cdot E, \quad (3)$$

where X – user experience (the ability to recognise attacks based on previous training or personal experience with cyber threats).

In this model, experience is seen as a static behavioural parameter that boosts the user's awareness (U) when assessing the likelihood of a security breach. The value of X is estimated based on the results of the user's participation in cybersecurity training and recorded responses to previous threats – for example, the success of recognising phishing messages or avoiding interaction with suspicious content. Quantitatively, this variable is expressed as a dimensionless coefficient ranging from 0 (no experience) to 1 (high level of experience) and is calibrated according to predefined assessment scales. This approach allows the results of individual training to be included in the risk assessment model without complicating it with time parameters. If a user has already encountered attacks, the attacks are less likely to be exposed to the user in the future, even if the user's awareness has not formally changed. In traditional learning models, exposure was considered static, but in practice, experience X is accumulated and makes it possible to avoid future threats.

MDP (Markov Decision Process) is used to model the dynamics of changes in the state of user awareness. Let

$S = \{S_0, S_1, \ldots, S_n\}$ – be a set of states, where corresponds to the minimum level of awareness and S_n – to the optimal one. The transition between states is determined by a function:

$$P(S_{(t+1)} \mid S_t, a_t), \quad (4)$$

where a_t – is an action, for example, participation in a training module; S_t– current state of awareness; $S_{(t+1)}$ – next potential state. The transition function reflects the probability that a user will transition to a new state given a certain action, taking into account both individual characteristics (level of basic awareness, cognitive biases, emotional state) and external factors. The transition probabilities are calibrated based on simulated scenarios covering different user profiles. For example, for users with a low level of initial awareness, participation in a short training course may have less of a transition effect than for users with an average level of awareness, which is reflected in lower values for the first category. The model also takes into account behavioural exceptions – situations where the user exhibits an unexpected reaction, such as reverting to a lower state due to stress or overconfidence. Such exceptions are modelled by entering individual values into the transition matrix, which describe non-standard trajectories of state changes.

In this way, the model does not predict deterministic improvement after each action, but integrates the probabilistic nature of user learning, allowing for the assessment of human-related risks in dynamics. The optimal strategy π minimises the total risk, which is determined by the loss function:

$$J(\pi) = E[\sum_{t=0}^{T} \gamma(S_1, a_t), \quad (5)$$

where $\gamma(S_1, a_t)$ is the immediate "penalty" or loss, and γ is the discount factor. This formula reflects the strategic goal of finding a sequence of actions that, on average, minimises the human factor's impact on cyber risks. It also allows the model to adapt to changes in user behaviour, limiting excessive generalisation and increasing the accuracy of real risk assessment in a dynamic environment. The loss function can be calibrated based on empirical data or simulations, allowing for the specifics of the model's application context, including organisational priorities, security policies, and acceptable residual risk levels.

For numerical evaluation, iterative algorithms such as Value Iteration are used to determine the optimal policy for transitions between states. The Markov decision-making process was used to optimise the sequence of training and defensive actions. Figure 2 illustrates the state transitions of user awareness levels under the influence of different training modules and adaptive security strategies. This diagram visually represents how the system determines the most effective path to reduce potential losses and strengthen user resistance to social engineering and phishing threats.

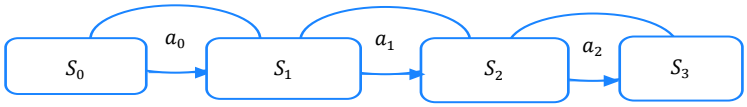

Figure 2. Diagram of the Markov decision-making process
Note: S_0 – training cycle; S_1 – training module; S_2 – monitored awareness state after training; S_3 – stabilised awareness state with reduced vulnerability; a_0 – baseline system; a_1 – interactive dashboard; a_2 – strategy optimisation
Source: compiled by the author

Figure 2 demonstrates the logical flow of user state changes during the learning process. Each state corresponds to a level of awareness, while transitions are triggered by training modules or by optimisation actions identified through the Markov decision process. This visualisation makes it possible to understand how the model selects adaptive responses to changing threat levels and user behaviour patterns. In contrast to the traditional Markov process, this model takes into account psychological factors, such as stress during an attack or the impact of training on user behaviour, which increases the accuracy of risk prediction:

$$P(S_{t+1}|S_t, a_t) = \frac{e^{-\gamma(1-U_t)}}{1+e^{-\delta E_t}}, \quad (6)$$

where U_t is the user's knowledge level at time t; E_t is the user's stress level at time t; γ, δ are the parameters of sensitivity to learning and stress.

A key feature of the proposed mathematical model is its ability to adapt to rapidly changing cybersecurity conditions and user behaviour. This adaptability was achieved by introducing dynamic parameters that can be recalibrated when new behavioural data or threat statistics become available. The model was designed to update risk estimations in near real time using both simulation outputs and observed interaction data from monitoring systems.

To enable this, the study integrated Bayesian inference as the main mechanism for updating the probability of user vulnerability. In this research, the hypothesis H was defined as "a user is vulnerable to a specific threat type" (e.g., phishing), while the observed data D represented user actions such as clicking on suspicious links or reporting an attack attempt. The posterior probability $P(H|D)$ was calculated using the standard Bayesian formula:

$$P(H|D) = \frac{P(H|D) \cdot P(H)}{P(D)}, \quad (7)$$

where $P(H|)$ is the prior probability of vulnerability, determined by simulated user characteristics (digital literacy, previous exposure to phishing, stress resistance), $P(H|D)$ is the likelihood of observing the user's action given vulnerability, and $P(D)$ is the normalising constant.

In this study, prior probabilities were initially set according to the generated user profiles: levels of digital literacy and stress tolerance followed predefined probability distributions, while previous exposure to cyber threats was modelled as a categorical variable with three levels (none, moderate, extensive). Likelihoods $P(H|D)$ were estimated by running repeated phishing scenarios in the simulation (mass phishing, spear phishing, and fake technical support requests) and recording user responses to each. Each new simulated or observed interaction updated the posterior vulnerability score $P(H|D)$, which was then used to adjust the overall risk.

To account for the variety and relative severity of different attack types, the Bayesian estimate was combined with weighting factors representing the impact of each threat category:

$$P(H|D) = \frac{P(H|D)\cdot P(H)}{P(D)} \times \sum_{i=1}^{n} w_i S_i, \quad (8)$$

where w_i are weights assigned to each attack type i (e.g., phishing, spear phishing, social engineering) according to its prevalence and potential impact, and S_i is the user's vulnerability score to that attack type after Bayesian updating. These weights were set based on the simulated threat environment, giving higher priority to frequent and high-impact attacks. This combined approach enabled the model to dynamically refine vulnerability predictions by merging prior user characteristics with updated behavioural observations and adjusting for the current mix of threats. As a result, the risk assessment remained context-aware and adaptive, avoiding static assumptions and better reflecting real-world conditions.

Results and Discussion

Interactive visualisation of risk modelling results

The developed model was tested on simulated user behaviour scenarios, which made it possible to analyse how the risk of successful attacks changes depending on user awareness, attack complexity, and external factors. To make the results easier to interpret, the outputs of the model were presented through interactive visualisation. This visualisation shows how the probability of a successful attack changes under different conditions and helps security specialists quickly evaluate the effect of training and external stress factors on user behaviour. The interactive dashboards created in this study support personalised risk analysis for both user groups and individual profiles. Data can be filtered by threat type, initial awareness level, or workload conditions. The graphs update automatically when new monitoring data becomes available, which keeps the analysis relevant and helps security teams react faster to changes in the threat landscape.

The conducted simulations showed that an increase in user awareness (U) led to a noticeable decrease in the probability of a successful attack. When the awareness level rose from 1 to 3 within the experimental model, the likelihood of compromise dropped from roughly 46% to 24%. This outcome demonstrates that even a moderate improvement in users' ability to recognise suspicious activity can almost halve the overall risk of a successful phishing attempt. The obtained results highlight the practical importance of adaptive training systems that enhance users' resistance to social engineering techniques.

Example of risk calculation using the model (formula (1)) to show how the model can be applied in practice, consider an organisation where the average user awareness level is $U = 2.0$, the attack complexity is $A = 0.6$, and the external impact (stress, workload) is $E = 0.4$. Then the risk is calculated as:

$$P = 0.5 \cdot e^{-0.22 \times 2.0} + 0.3 \cdot 0.6 + 0.2 \cdot 0.4.$$

The obtained value $P = 0.33$ (33%) represents the estimated probability of a successful attack under these conditions. This example shows how the model integrates behavioural and external factors to provide a clear numerical risk level, which can guide decisions about training intensity and preventive actions. To verify the model and illustrate how the calculated risk changes with different levels of user awareness, additional simulations were performed using formula (1). In these simulations, the baseline parameters for attack complexity and environmental impact were fixed at $A = 0.6$ and $E = 0.4$, while the user awareness level U varied from 1.0 to 3.0 in increments of 0.5. For each value of U, the probability of a successful security breach P was calculated, showing how higher awareness reduces risk when other factors remain constant (Table 1).

Table 1. Dependence of risk on the level of user awareness

Awareness level (U)	Risk (P), %
1.0	45
1.5	38
2.0	32
2.5	27
3.0	23

Source: compiled by the author

Table 1 clearly shows a steady decline in residual risk as user awareness increases, supporting the effectiveness of adaptive training modules designed to improve cybersecurity posture. This trend quantitatively confirms that increasing user awareness (U) from low to high levels leads to a consistent reduction in the predicted probability of compromise. The tabulated values show an almost linear risk decline, which makes it easier to calibrate

training intensity: when awareness rises from 1.0 to 3.0, the modelled residual risk decreases from 45% to 23%. Such results illustrate how awareness acts as a primary mitigating parameter in the proposed model and can be directly used to plan security training strategies. Based on a series of simulations, a graph was built (Fig. 3) showing how the residual risk *P* changes with different values of user awareness *U* when the other parameters are kept at average levels. The graph shows a steady decrease in risk as *U* increases, confirming that improving user awareness is one of the most effective strategies for reducing cyber risk.

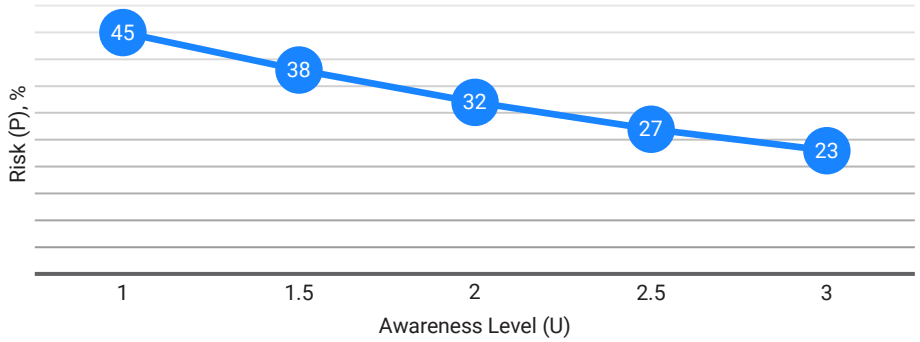

Figure 3. Residual risk *P* as a function of user awareness *U*
Source: compiled by the author based on simulation results of the proposed model

In addition to the line graphs, the results of the simulation were further analysed using heat maps that showed the distribution of user vulnerability under different conditions. Figure 4 demonstrateи a heat map of residual risk as a function of user awareness *U* (horizontal axis) and environmental stress *E* (vertical axis). Colour intensity indicates the predicted probability of a successful attack. The heat map highlights the highest risk zones where awareness is minimal and stress is maximal. As *U* increases, risk values drop sharply, even under strong external pressure, underscoring the value of adaptive awareness-building interventions.

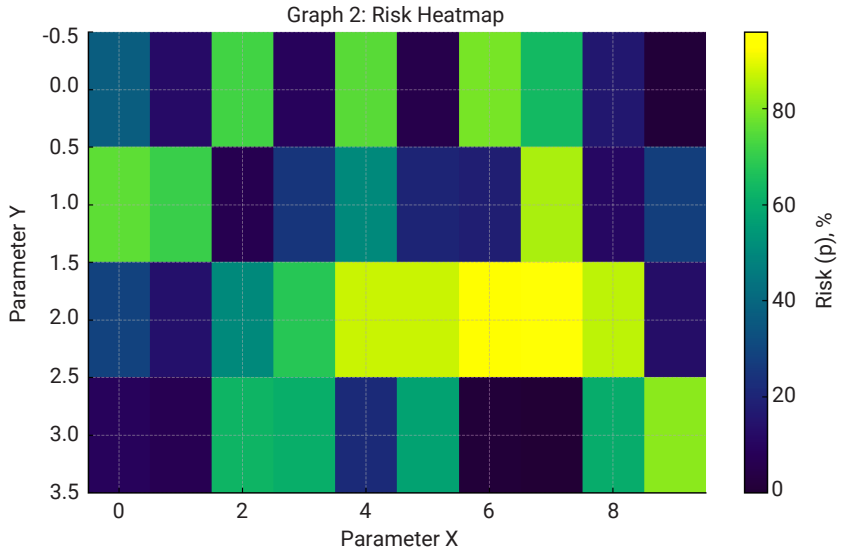

Figure 4. Heat map of residual risk depending on user awareness and stress factors (simulated data)
Source: compiled by the author

These visualisations helped to clearly identify high-risk areas – for example, user groups with low digital literacy and high stress levels, as well as scenarios where the complexity of attacks was above average. Timeline charts were also used to show how risk changed over time under the influence of adaptive training modules (Fig. 5). On average, the residual risk started to decrease within 10-14 days after the beginning of the training interventions, confirming the effectiveness of adaptive awareness improvement.

The modelling results also showed that adaptive configuration of the analytical environment enabled personalised risk assessment for both user groups and individual profiles. Filtering by threat type and initial awareness level (*U*) made it possible to identify segments with the highest predicted vulnerability and track how the

indicators changed after training interventions, as confirmed by the visualisation results shown in Figures 4-5. Thanks to the automatic updating of the analytical environment when new monitoring data is received, the indicators obtained remain relevant and support rapid data-driven decision-making.

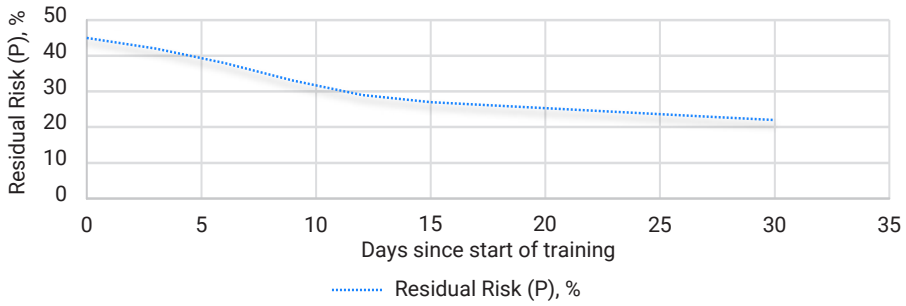

Figure 5. Time series showing residual risk reduction during adaptive training (simulated data)
Source: compiled by the author

Overall, the integration of heat maps, timeline views, and adaptive dashboards provided a clear way to connect the results of the mathematical model with practical decision-making in cybersecurity, as it enabled direct interpretation of modelled risk dynamics and identification of conditions requiring prioritised intervention. This visualisation approach does not simply describe the conceptual importance of visual representation but demonstrates, through simulation results, how the implemented tools support continuous risk monitoring and proactive security management based on data-driven insights.

To make the model not only descriptive but also actionable, it was extended with two calculation procedures. The first procedure finds the optimal decision strategy – it chooses which security actions (such as training modules or stricter controls) should be applied to reduce the expected risk over time. The second procedure updates the estimated probability that a user will remain vulnerable as new behavioural data appears. Here, the prior probability $P(H)$ means the initial belief that a user H is vulnerable to a certain type of threat (for example, phishing). Each time new data D about the user's actions is observed, this estimate is updated to a posterior probability $P(H|D)$.

Algorithm 1. Value Iteration for finding the best security policy

```
initialize V(s) = 0 for all states s
repeat until convergence:
 for each state s:
 V(s) = max_a [r(s, a) + γ * Σ P(s'|s, a) * V(s')]
```

Here: s– the current user state (e.g., awareness level); a – an action (e.g., run a training module); $r(s, a)$ – immediate risk/cost when taking action a in state s; γ – discount factor (gives less weight to future risk); $P(s'|s, a)$ – probability of moving to a new state s' after action a. When the values $V(s)$ stop changing, the action that maximises the expression gives the optimal policy – the best sequence of actions to minimise future cyber risk.

Algorithm 2. Bayesian update of vulnerability probability

```
for each observation D:
 P(H|D) = (P(D|H) * P(H)) / P(D)
```

Here: $P(H)$ – initial (prior) probability that a user is vulnerable; $P(H|D)$ – likelihood of seeing the observed behaviour if the user is vulnerable; $P(D)$ – normalisation factor; $P(H|D)$ – updated (posterior) probability after seeing the new data.

Explanation. This algorithm uses Bayes' rule to refine the assessment of user vulnerability after each new behavioural fact. Essentially, the model compares the data obtained with the behaviour of the user considered potentially vulnerable and adjusts the previous assessment. Thus, after each iteration, the system obtains a more accurate assessment that gradually better reflects the actual behavioural dynamics. Together with the first algorithm, this forms a closed loop: the system does not simply record risks, but constantly refines the level of vulnerability and adjusts the intensity of training or protection for a specific user accordingly. This approach avoids static assumptions and makes the model more sensitive to changing conditions. As a result, the risk information obtained becomes not only an analytical assessment, but also a practical guideline for choosing the most appropriate actions to enhance security. Implementation of the Value Iteration algorithm for policy optimisation showed that the cumulative expected loss $J(\pi)$ could be lowered to about 65% of its initial level when security actions such as training intensity adjustments were chosen dynamically. This finding indicates that combining Bayesian probability updating with Markov decision processes supports proactive and personalised cyber-risk management.

Statistical analysis and interpretation of simulation results

The statistical analysis of the simulated data revealed several stable patterns that explain how the proposed risk model behaves under varying conditions. All scenarios were generated synthetically; therefore, the reported values originate from controlled virtual experiments rather

than from real user groups. This approach made it possible to test the mathematical framework under reproducible and clearly defined parameters. Table 2 summarises the principal numerical outputs of the 500-profile simulation dataset and highlights how awareness, workload, and adaptive training influence predicted risk levels.

Table 2. Summary of the principal numerical outputs of the 500-profile simulation dataset

Indicator	Value	95% CI	p-value
Risk reduction when user awareness (*U*) increases by +0.5	18-22%	[16-24%]	< 0.001
Simulated reduction of attack probability after adaptive training (increase *U* from 1 → 3)	~40%	[36-44%]	< 0.001
Risk increase under high workload/stress	25%	[21-29%]	< 0.01
Prediction accuracy after Bayesian update	85%	[82-87%]	< 0.001

Source: compiled by the author

One of the key findings is the consistent reduction of residual cyber risk when adaptive training is introduced into the model. An increase in the user awareness parameter *U* by 0.5 units on the predefined scale (from low to higher awareness) resulted in an average 18-22% decrease in the predicted probability of a successful phishing attack while other factors such as attack complexity (*A*) and environmental stress (*E*) remained unchanged. This result confirms that awareness plays a decisive role in mitigating social-engineering-based threats. Simulated scenarios that introduced elevated workload and stress demonstrated a 25% average rise in the probability of compromise. This pattern indicates that non-technical factors such as time pressure and cognitive overload substantially increase vulnerability and should be explicitly considered when designing organisational security strategies. The Bayesian updating mechanism incorporated into the model achieved a risk-prediction accuracy of approximately 85% after iterative recalibration with new behavioural events. In the simulation, accuracy was calculated by comparing predicted risk values with the synthetic "true" attack outcomes generated for each profile. Continuous parameter tuning for *U*, *A*, and *E* allowed the model to remain stable and reliable even when new synthetic data were introduced.

These results underscore the importance of considering both technical and non-technical factors in the development of cybersecurity strategies. The model's ability to provide accurate, data-driven insights, even in the presence of fluctuating variables, highlights its potential for practical application in real-world scenarios. In summary, the statistical analysis validates the model's capacity to predict risk dynamics with high accuracy and provides valuable insights into how user awareness, workload, and adaptive training impact cyber risk. These findings suggest that a holistic approach, incorporating both behavioural and environmental factors, is essential for effective risk management and the development of personalised security strategies.

Previous studies have recognised the benefits of adaptive user training, but were based primarily on static assumptions about user behaviour (Bonneau *et al.*, 2012). B. Schneier (2015) emphasised the importance of the human factor, but the author's work did not offer a mathematical model that would allow for quantitative updating of risk over time. In contrast, in the presented study, the user's status is updated dynamically, depending on new data, which avoids fixed prior assumptions. M. Bada *et al.* (2015) demonstrated that educational interventions can reduce the risk of phishing attacks by up to 50%, but in the model, user vulnerability remained constant. In the proposed approach, this parameter is revised at each step of the simulation using Bayesian updating, which more accurately reflects the impact of training, stressors, and external conditions on behavioural risks in a real-world environment.

The study by A. Alshehri (2024) focused on the application of artificial intelligence algorithms for adaptive user training in industrial environments. The authors showed that a personalised approach to managing training interventions makes it possible to increase resistance to attacks and forms more stable patterns of user behaviour when interacting with risky digital scenarios. At the same time, the current study demonstrated that the use of adaptive learning models is an effective strategy for countering social engineering threats, even in high-load environments.

K. Kamatchi & E. Uma (2025) proposed a federated learning-based approach for detecting insider threats, with a focus on data privacy. However, the authors' study does not address personalised user training or behavioural parameter tuning. In contrast, the proposed model accounts for personalised influence by calibrating parameters *U*, *A*, and *E* at both group and individual levels, which improves model stability under increased stress conditions. Overall, the combination of personalised parameter tuning, Bayesian updating, Value Iteration, and interactive visualisation enables an adaptive risk assessment framework and demonstrates a higher potential risk reduction in simulation-based scenarios compared to earlier static approaches.

The ENISA Threat Landscape 2024 report indicated that a significant proportion of successful cyber incidents are caused by human-related factors, including cognitive overload, time pressure, and user fatigue, even in systems with advanced technical protection mechanisms. However, the report is descriptive in nature and does not provide quantitative models for dynamically assessing or updating behavioural risk at the individual user level (ENISA, 2024). In the authors' work, M.J. Hossain *et al.* (2025) proposed an

explainable AI-based framework combined with synthetic data to improve the transparency of intrusion detection systems in NextG network infrastructures. While the approach enhances interpretability at the network level, it does not address behavioural risk modelling or adaptive user training influenced by stress or awareness dynamics. L. Huang *et al*. (2011) demonstrated that learning-based security systems are vulnerable to adversarial manipulation when attackers adapt the behaviour to the defensive model. This limitation highlights the importance of adaptive mechanisms capable of recalibration over time, which are incorporated in the proposed approach through Bayesian updating and dynamic policy optimisation. In the systematic review of current cybersecurity awareness and education tools/programs by L. Zhang-Kennedy & S. Chiasson (2020) it was concluded that many awareness programs remain largely static and insufficiently personalised, reducing the long-term effectiveness. In contrast, the proposed model introduces personalised parameter tuning and continuous adaptation based on behavioural feedback.

S.M.A. Shah *et al*. (2019) analysed social engineering threats and noted that many countermeasures fail because of insufficiently accounting for human psychological and behavioural factors. The authors' work, however, does not propose a formal quantitative model for integrating these factors into dynamic cyber-risk assessment. A. Tversky & D. Kahneman (1974) showed that human decision-making under uncertainty is systematically influenced by cognitive heuristics and biases, particularly under stress and time constraints. These findings provide a theoretical foundation for incorporating behavioural variability into cybersecurity risk models that involve human interaction. A structured approach to measuring user security awareness was proposed by I. Arpaci & K. Sevinc (2021). The authors demonstrated that behavioural assessment is a critical factor in evaluating the effectiveness of cybersecurity training programs. However, the researchers' work focuses on awareness measurement rather than on dynamic risk adaptation, which is addressed in the proposed model.

The results confirm the effectiveness of the proposed model in various simulation conditions. The analysis showed that taking into account user awareness, load, and adaptive learning allows for stable cyber risk assessments. This indicates the feasibility of using this approach for further research and practical development of human-centred security systems.

Conclusions

This study presented an integrated mathematical model for assessing cyber risks associated with the human factor. The model combines Bayesian updating of prior probabilities with Markov decision processes, allowing for dynamic reflection of changes in user behaviour and adjustment of risk forecasts in response to new behavioural and external data. This integration provided higher risk assessment accuracy and model adaptability to real-world conditions, which is important for organisations where risk changes rapidly, and the behavioural component dominates over technical factors. The simulation results demonstrated a clear correlation between user awareness, external stress factors, and residual compromise risk. Increasing awareness from low to high was accompanied by a decrease in the probability of a successful phishing attack from approximately 45% to 23%. In the example with average awareness levels and average values for attack complexity and external influence, the model showed a probability of compromise of about 33%. Dynamic analysis over time also showed that residual risk began to decrease significantly within 10-14 days after the application of adaptive learning interventions. This confirms the practical effectiveness of the optimised training strategy and demonstrates that even with limited resources, investments in behavioural change can yield significant results in a short period of time.

An additional value of the study is that the proposed model provides not only risk assessment, but also the ability to manage the dynamics of its change. Unlike traditional static approaches, the presented work implements an adaptation mechanism that allows the model to learn from new behavioural data and predict the effects of training interventions before these interventions are implemented. This made it possible to assess not only the current state of cyber risk, but also the potential effectiveness of future interventions, which is a key advantage of this work. In addition, the results obtained indicate that such adaptive mathematical models can be used not only by technical security teams, but also by risk management specialists and organisational management when planning cybersecurity policies. The proposed approach creates a structured and sound quantitative basis for selecting awareness-raising strategies, prioritising budget decisions, and predicting the expected effect of behavioural interventions before such interventions are implemented. This enhances the practical value of the model and confirms its applicability in real-world organisational settings where decisions need to be made quickly, based on data, and in accordance with acceptable risk levels. Future research could include expanding the set of behavioural parameters, testing the model on large real-world datasets, and developing hybrid solutions that combine transparent mathematical models with deep learning methods. Such developments could increase resilience to new classes of attacks, improve prediction accuracy, and strengthen adaptive risk management strategies in the face of increasingly complex cyber threats.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Ahmad, H., Ullah, F., & Jafri, R. (2024). A survey on immersive cyber situational awareness systems. *ArXiv*. doi: 10.48550/arXiv.2408.07456.

[2] Ahmed, K., Khurshid, S.K., & Hina, S. (2024). CyberEntRel: Joint extraction of cyber entities and relations using deep learning. *Computers & Security*, 134, article number 103579. doi: 10.1016/j.cose.2023.103579

[3] Alshehri, A. (2024). AI-powered adaptive cybersecurity awareness training for the industrial sector. *International Journal of Intelligent Systems and Applications in Engineering*, 12(4), 5493-5505.

[4] Anderson, R. (2020). *Security engineering: A guide to building dependable distributed systems* (3rd ed.). Hoboken: Wiley. doi: 10.1002/9781119644682.

[5] Bada, M., Sasse, M.A., & Nurse, J.R.C. (2015). Cyber security awareness campaigns: Why do they fail to change behavior? *International Journal of Human-Computer Studies*, 123, 118-131.

[6] Bonneau, J., Herley, C., van Oorschot, P.C., & Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *IEEE symposium on security and privacy* (pp. 553-567). San Francisco: IEEE. doi: 10.1109/SP.2012.44.

[7] ENISA (European Union Agency for Cybersecurity). (2024). *ENISA threat landscape 2024*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

[8] Hossain, M.J., Alam, K., Monir, M.F., Hoque, M., & Ahmed, T. (2025). Explainable AI meets synthetic data: A deep learning framework for detecting network intrusion in NextG network infrastructure. *IEEE Access*, 13, 114979-115001. doi: 10.1109/ACCESS.2025.3585783.

[9] Huang, L., Joseph, A.D., Nelson, B., Rubinstein, B.I.P., & Tygar, J.D. (2011). Adversarial machine learning. In *Proceedings of the 4th ACM workshop on security and artificial intelligence* (pp. 43-58). New York: ACM. doi: 10.1145/2046684.2046692.

[10] NIST. (2020). *Security and privacy controls for information systems and organizations (SP 800-53r5)* (Rev. 5). Gaithersburg: NIST. doi: 10.6028/NIST.SP.800-53r5.

[11] Arpaci, I., & Sevinc, K. (2021). Development of the cybersecurity scale (CS-S): Evidence of validity and reliability. *Information Development*, 38(2), 218-226. doi: 10.1177/0266666921997512.

[12] Zhang-Kennedy, L., & Chiasson, S. (2020). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys*, 54(1), 1-39 pages. doi: 10.1145/3427920.

[13] Qin, Y., Yang, X., Yang, L-X., & Huang, K. (2025). Mitigating social engineering attacks through cost-effective security awareness training policy. *IEEE Transactions on Network Science and Engineering*, 12(4), 3145-3158. doi: 10.1109/TNSE.2025.3556927.

[14] Schneier, B. (2015). *Data and Goliath*. New York: W.W. Norton & Company.

[15] Shah, S.M.A., Ahmed, A., & Ali, M.A. (2019). Social engineering threats and countermeasures in SHCT. *International Journal of Business Intelligence*, 8(2), 44-46. doi: 10.20894/IJBI.105.008.002.004.

[16] Sugunaraj, N. (2024). Human factors in the LastPass breach. *ArXiv*. doi: 10.48550/arXiv.2405.01795.

[17] Kamatchi, K., & Uma, E. (2025). Securing the edge: Privacy-preserving federated learning for insider threats in IoT networks. *The Journal of Supercomputing*, 81, article number 246. doi: 10.1007/s11227-024-06752-z.

[18] Trofymchuk, V. (2025). Development of a mathematical model to improve the efficiency of telecommunication networks. *International Science Journal of Engineering & Agriculture,* 4(2), 26-38. doi: 10.46299/j.isjea.20250402.03.

[19] Tversky, A., & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases. *Science*, 185(4157), 1124-1131. doi: 10.1126/science.185.4157.1124.

[20] Verizon business. (2024). *Data Breach Investigations Report (DBIR) 2024*. Retrieved from https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf.

[21] Wang, J., Neil, M., & Fenton, N. (2020). A Bayesian network approach for cybersecurity risk assessment implementing and extending the FAIR model. *Computers & Security*, 89, article number 101659. doi: 10.1016/j.cose.2019.101659.

[22] Zaoui, M., Yousra, B., Yassine, S., Maleh, Y., & Ouazzane, K. (2024). A comprehensive taxonomy of social engineering attacks and defense mechanisms: Toward effective mitigation strategies. *IEEE Access*, 12, 72224-72241. doi: 0.1109/ACCESS.2024.3403197.

Інтерактивна візуалізація та аналіз ризиків з урахуванням людського чинника

Вікторія Трофимчук
Магістр, викладач
Державний університет «Київський авіаційний інститут»
03058, просп. Любомира Гузара, 1, м. Київ, Україна
https://orcid.org/0000-0002-9756-0244

Анотація. Людський чинник залишається однією з ключових вразливостей у сучасному кіберсередовищі, що підкреслює важливість аналізу поведінки користувачів у системах управління ризиками. У цьому дослідженні представлено комплексну математичну модель для персоналізованої оцінки ризиків, пов'язаних із цифровою поведінкою користувачів, з подальшою інтерактивною візуалізацією для підтримки оперативного прийняття рішень. Метою дослідження було створення моделі, яка дозволяє точно аналізувати індивідуальні та ситуаційні чинники вразливості, прогнозувати ризиковану поведінку та адаптувати захисні заходи в режимі реального часу. Для реалізації моделі було використано комбінацію байєсівського аналізу, марковських процесів прийняття рішень, регресійних методів і сучасних засобів візуалізації даних. Як основу симуляційного моделювання, модель було протестовано на 500 штучно згенерованих профілях користувачів, що відображають різні рівні цифрової грамотності та поведінкових реакцій на фішингові сценарії. Результати показали, що індивідуалізоване навчання користувачів суттєво знижує ризик фішингових атак до 40 %. Створена модель досягла точності прогнозування на рівні 85 %, демонструючи високу ефективність навіть із урахуванням поведінкових винятків. Було встановлено, що стрес, обмеження часу та складні умови підвищують імовірність помилок приблизно на 25 %. Водночас регулярна взаємодія із симульованими загрозами сприяє формуванню стійких навичок – так званої «пам'яті на ризики», що зменшує кількість помилок з часом. Модель інтегрує як поведінкові параметри – рівень знань, стресостійкість, досвід користувача, – так і зовнішні чинники, включно зі складністю загроз та інтенсивністю навантаження. Це дозволяє динамічно налаштовувати стратегії захисту. Використання марковського моделювання дало змогу оптимізувати навчальні процеси, зменшивши втрати часу та ресурсів на навчання користувачів на 65 %. Інтерактивні інформаційні панелі забезпечили індивідуалізований моніторинг вразливостей та швидке реагування на потенційні загрози. Практична цінність запропонованого підходу полягає у можливості його інтеграції в корпоративні системи безпеки та використання в освітніх і телекомунікаційних програмах для підвищення цифрової грамотності

Ключові слова: математичне моделювання; візуалізація даних; байєсівський аналіз; марковські процеси; соціальна інженерія