Journal of Further and Higher Education

Journal of Further and Higher Education

ISSN: 0309-877X (Print) 1469-9486 (Online) Journal homepage: www.tandfonline.com/journals/cjfh20

ProtectTech: a ChatGPT generated scenario activity to foster student decision-making capability

Jordan Allison

To cite this article: Jordan Allison (2026) ProtectTech: a ChatGPT generated scenario activity to foster student decision-making capability, Journal of Further and Higher Education, 50:1, 25-48, DOI: 10.1080/0309877X.2025.2583091

To link to this article: https://doi.org/10.1080/0309877X.2025.2583091

Published online: 06 Nov 2025.

JOURNAL OF FURTHER AND HIGHER EDUCATION
2026, VOL. 50, NO. 1, 25–48
https://doi.org/10.1080/0309877X.2025.2583091

Routledge
Taylor & Francis Group

OPEN ACCESS
Check for updates

ProtectTech: a ChatGPT generated scenario activity to foster student decision-making capability

Jordan Allison

School of Business, Computing, and Social Sciences, University of Gloucestershire, Gloucestershire

ABSTRACT
Cyber security and political science are increasingly becoming interconnected, and from this an interdisciplinary skillset is emerging. This calls for the importance of effective education to foster the development of these skills. Drawing on the importance of engaging and applied learning experiences, this paper introduces ProtechTech Solutions, a scenario-based group activity generated by ChatGPT. The scenario is presented, and how it was used for a group of postgraduate students studying 'Information Security Management'. Addressing the integration of ChatGPT into teaching practices, the paper fills a research gap by demonstrating how large language models can efficiently create classroom resources and lead to increased student engagement, measured through the variables of interest and excitement. Therefore, this paper provides a concrete example of practice, offering instructors valuable insights into adopting similar strategies. Furthermore, it was found that the scenario activity contributed to increased student self-efficacy and the development of essential skills, including decision-making, critical thinking, communication, and teamwork. These skills, crucial for both cybersecurity specialists and political scientists, transcend various domains globally, suggesting the adaptability of ProtechTech's scenario creation process to other subject areas.

ARTICLE HISTORY
Received 28 December 2023
Accepted 26 October 2025

KEYWORDS
Scenario-based learning; cyber security; decision-making; ChatGPT

Introduction

The relationship between cybersecurity and political science reflects the growing significance of the digital domain in global politics and governance (Cavelty and Wenger 2020). This interdependence not only heightens national security concerns but also necessitates interdisciplinary education that prepares professionals capable of navigating both technical and political dimensions of cyber threats. Central to this connection lies the imperative of safeguarding national security, where cybersecurity assumes a pivotal role in protecting digital infrastructure, sensitive information, and communication systems from cyber threats. Indeed, one of the key knowledge domains in cybersecurity, according to the CyberSecurity Body of Knowledge (CyBOK), is Law and Regulation, which is stated as including 'International and national statutory and regulatory requirements, compliance obligations, and security ethics, including data protection and developing doctrines

CONTACT Jordan Allison jrallison@hotmail.co.uk School of Business, Computing, and Social Sciences, University of Gloucestershire, The Park, Cheltenham GL50 2RH, Gloucestershire

on cyber warfare' (Martin et al. 2021). Cyberattacks, with their potential geopolitical implications, have become integral instruments in international relations and political conflicts, highlighting the complex link between cybersecurity and state security concerns.

Within the realm of international relations, cybersecurity issues permeate discussions on cyber espionage, warfare (Cavelty and Wenger 2020), and public attribution (Egloff 2020). Qian (2019) discusses the relationship between the U.S. and China and outlines how restrictive measures have been taken by the U.S. about trade based on 'cyberspace security'. Additionally, cyber warfare, involving digital attacks to disrupt or disable another state's infrastructure, is becoming more common. Praprotnik, Ivanuša, and Podbregar (2013) and Naugle, Bernard, and Lochard (2016) outline how a distributed denial of service attack in 2007 caused huge economic damage in Estonia, while the commonly known Stuxnet Worm, was originally aimed at destroying Iran's nuclear facilities (Fidler 2011; Masood et al. 2011; Stevens 2020). More recently, there was the 2017 WannaCry ransomware attack on the United Kingdom National Health Service (Aljaidi et al. 2022), while in the US, the 2021 ransomware attack on the Colonial Pipeline significantly affected national infrastructure due to its influence on restricting oil supply (Beerman et al. 2023).

Election security is another domain where the interplay between cybersecurity and political science is substantial (Toapanta, Briones Peñafiel, and Enrique Mafla Gallegos 2020). Ensuring the integrity of elections is a paramount concern, necessitating robust cybersecurity measures to protect election systems from hacking, manipulation, and other cyber threats (Metcalf 2021). From as early as 2010, some authors have discussed the importance of having cybersecurity professionals on policy boards to assess online-based election processes (Hoke 2010), but issues persist. For instance, leaked sensitive documents at the 2016 U.S. presidential election highlighted the growing threat of interference to democratic processes and the legitimacy of political outcomes (Pope 2018).

Given the rise of attacks, governments enact laws and regulations to address cyber threats, safeguard critical infrastructure, and define the responsibilities of various stakeholders. This legislative process involves nuanced considerations of political power dynamics, national interests, and international cooperation. However, important to these policies is the consideration of the effects that any policy is having, and if they are for the public good (Stevens 2020). For instance, in striking a balance between cybersecurity efforts and the protection of individual rights. Hence, formulation and implementation of effective policies constitute a critical area where actors of political science require an understanding of cybersecurity, and cybersecurity professionals require an understanding of effective policy formulation.

In order to ensure there is sufficient expertise across both domains, this calls for the importance of education. Cybersecurity attacks have led to an increased need for cybersecurity professionals (Hajny et al. 2021; Ricci et al. 2021), but cybersecurity should not just be present in explicit cybersecurity programs, but across mainstream higher education (Parrish et al. 2018). Despite its growing relevance, there is limited formal scholarship exploring cybersecurity within political science and international relations education (Herr, Laudrain, and Smeets 2021). However, higher education providers are expanding their curricula to include cybersecurity components as part of political science courses (Herr, Laudrain, and Smeets 2021). Conversely, cybersecurity management and policy formulation are also becoming more prominent with explicit studies documenting examples of incorporating the management and policy aspects into cybersecurity curriculum design (Allison 2023a; Asghar and Luxton-Reilly 2020; Maguire, English, and Draper 2019). This development aligns with the 2017 Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity, which outline 'societal security' as a key knowledge area, including cybercrime, cyber law, cyber ethics, cyber policy, and privacy (Joint Task Force on Cybersecurity Education 2017). Overall, for effective interdisciplinary study, it is important to understand the skills that are present and required across both domain areas.

In parallel with curriculum reform and the increasing focus on interdisciplinary skill sets, educators have begun exploring the potential of generative artificial intelligence tools, such as ChatGPT, in higher education. Developed by OpenAI, ChatGPT is a large language model trained on extensive textual data and capable of generating human-like responses to natural language prompts (Ray 2023). Recent studies suggest its value as a pedagogical support tool, particularly in fostering critical thinking, personalised learning, and problem-solving skills (Urban et al. 2024). In cybersecurity education specifically, ChatGPT has been explored for its ability to simulate realistic threat scenarios, generate role-play content, and provide rapid formative feedback to students (Santhi and Srinivasan 2024). Within political science and international relations, its ability to model argumentation and policy perspectives makes it a promising tool for scenario-based activities (Ran and Yuyue Zeng 2024). However, effective integration requires careful instructional design to ensure the technology supports rather than substitutes the development of student competencies (Yang, Hsu, and Wu 2025). The following section explores the shared competencies across both fields and forms the basis for the pedagogical model utilising ChatGPT, which is presented later in the paper.

An interdisciplinary skill set

Across the domain areas of cybersecurity and political science, a common emphasis on critical thinking and decision-making emerges as a pivotal aspect of professional competence (Albert 2021; Grossman and Schortgen 2016). Analytical thinking, foundational in both disciplines, demands not only a critical examination of intricate systems and political dynamics but also an adeptness in making well-informed decisions based on these analyses. The ability to discern patterns, anomalies, and potential threats becomes a precursor to effective decision-making, reflecting a shared requirement for nuanced judgement in navigating the complexities of cybersecurity and the political landscapes.

Effective communication, a key skill in both domains (Grossman and Schortgen 2016), extends its influence to the decision-making process. Cybersecurity professionals must articulate complex technical information to diverse stakeholders to facilitate collective understanding and informed decision-making (Jones, Siami Namin, and Armstrong 2018). Similarly, political scientists rely on clear communication to convey intricate political analyses, influencing decision-makers in policy formulation or public discourse (Biziouras 2013). This underscores the interconnectedness of communication and decision-making as mutually reinforcing skills in both fields.

Ethical considerations further elevate the significance of decision-making skills in cybersecurity and political science. Ethical awareness has been identified as a key contextual skill required for the twenty-first century (Van-Laar et al. 2017). Professionals in these realms are tasked with making decisions that uphold high ethical standards, navigating privacy concerns, respecting confidentiality, and adhering to legal boundaries (Joint Task Force on Cybersecurity Education 2017). The ethical terrain in decision-making underscores the weight of choices that impact individuals, organisations, or even nations, requiring a delicate balance of moral considerations.

As cyber threats often transcend national borders, the adaptability cultivated in cybersecurity education becomes an asset in global cyber diplomacy (Joint Task Force on Cybersecurity Education 2017). Professionals with adaptive skills are better equipped to engage in international collaborations, share threat intelligence, and contribute to the development of global cybersecurity norms and standards. This collaborative approach is essential for fostering international cooperation in response to cyber threats.

The convergence of technical proficiency, ethical considerations, effective communication, and adaptability in both cybersecurity and political science demonstrates their shared focus on decision-making as a multifaceted skill. A good decision-making process is important for handling the tough, changing problems in cybersecurity and politics. Increasingly, educators are also exploring how digital tools like ChatGPT can serve as platforms for simulating such decision-making processes in a controlled, reflective learning environment (Khaled et al. 2024). By facilitating the drafting of incident responses, mock policy briefs, or simulated diplomatic dialogues, generative AI can help learners practice these interdisciplinary skills with real-time feedback (Casey 2024). In summary, the comprehensive skill set instilled in cybersecurity students not only enriches their individual careers but also plays a crucial role in enhancing the political landscape for cybersecurity on both a national and global scale. Integrating AI tools such as ChatGPT into the learning process represents one route through which these skills can be scaffolded and assessed in innovative ways. By producing well-rounded professionals with ethical considerations, effective communication skills, and strategic acumen, cybersecurity education becomes a cornerstone in building a resilient and secure political environment amidst the evolving challenges posed by cyber threats.

This article, therefore, outlines the design and implementation of a scenario tool called ProtectTech Solutions, which was used for educational purposes for a group of postgraduate cybersecurity students at a university in the United Kingdom. The scenario activity aimed to help develop cyber professionals with the skills that are required to enter the political arena, given the interdisciplinary skills that are required, such as decision making, critical thinking, communication, and teamwork. The research question guiding this work is: How can scenario-based activities, supported by tools such as ChatGPT, be designed and implemented to foster interdisciplinary skills necessary for cyber professionals engaging with political processes?

While this paper is situated within the interdisciplinary overlap of cybersecurity and political science, it also contributes to ongoing debates about the role of AI in higher education. The use of ChatGPT as part of the ProtectTech scenario tool is not merely a matter of convenience but part of a broader pedagogical shift. Generative AI tools are increasingly being explored for their capacity to facilitate reflective learning, simulate complex decision environments, and personalise feedback (Zhan and Yan 2025). In this sense, this paper not only applies AI within a classroom context but critically examines how such tools can support the cultivation of ethical, communicative, and strategic competencies in a politically sensitive cyber landscape. This contributes to emerging work on the affordances and limitations of generative AI for higher-order skills development in social and technical domains alike.

The remainder of the article is structured as follows. (1) A discussion will be presented on the pedagogical approach of using scenario-based learning activities for education, given their prominence in increasing student motivation, engagement, and hence learning (Shanks and Jack Zhang 2023). (2) Following this, the situational context of the ProtechTech scenario will be presented along with how scenarios were selected and drafted. (3) Next, an example scenario will be presented outlining its contents and associated features, and 4) details on how the scenario was used in the classroom. 5) Finally, the paper will outline observations and student feedback of the scenario task, with a discussion on how this feedback and scenario activity relate to existing reports of practice.

Scenario-based learning activities

Scenario-related exercises are a pedagogical approach offering a dynamic and immersive tool for cultivating a spectrum of skills essential for future professionals in the field (Biziouras 2013; Shanks and Jack Zhang 2023). These exercises, which recreate real-world cyber threats or political decisions in a simulated environment, play a pivotal role in fostering decision-making, risk management, adaptability, ethical considerations, communication, and strategic planning skills (Garrison, Redd, and Carter 2010; Hazari 2005).

The incorporation of scenario-related exercises is paramount for various reasons. Primarily, simulation or scenario-based activities can promote active learning and increase student engagement (Hendrickson 2021; Shanks and Jack Zhang 2023). Hence, by ensuring students are engaged in their learning, these exercises provide effective and realistic preparation for incident response. By immersing students in simulated cyber incidents, they gain hands-on experience that enhances their ability to respond swiftly and effectively to actual threats. Furthermore, scenario exercises facilitate the practical application of risk management principles within a dynamic setting. Students are exposed to diverse risks, prompting them to evaluate potential consequences and make decisions under pressure. This experiential learning is invaluable for shaping their risk assessment skills, influencing future policy decisions, and contributing to a nation’s overall resilience against cyber threats.

The ever-changing nature of cyber threats demands an adaptive mindset, and scenario-based exercises provide a platform for adaptive problem-solving (England, Nagel, and Salter 2020). By presenting students with new and evolving challenges, these exercises foster the adaptability required to stay ahead of emerging threats and navigate the complexities of global cyber diplomacy (Biziouras 2013). Ethical considerations are seamlessly integrated into scenario exercises, requiring students to navigate complex situations with moral implications. Making ethical decisions in these simulated scenarios prepares students for the ethical dilemmas they may face in their professional roles. Moreover, the scenarios themselves can make students more aware and sensitive to the complexity of problems that may occur (Schoettmer 2023).

Effective communication is a key element in high-stakes situations, and scenario exercises create simulated stress environments that challenge students to articulate their decisions and strategies clearly (Schoettmer 2023). This experience enhances their communication skills, ensuring they can convey complex technical information to various stakeholders during real incidents should they occur. Moreover, the integration of strategic planning within simulated environments shapes students' decision-making processes, aligning them with overarching objectives (Garrison, Redd, and Carter 2010). This prepares students for the complexities of formulating policies, contributing to a nation's overall resilience against cyber threats.

Cyber conflict is a necessary topic to be covered for students of international relations, but it can be relatively inaccessible (Whyte 2021). Therefore, scenario exercises that simulate cyber conflicts contribute to students' preparedness for geopolitical tensions in the digital domain. Whyte (2021) outlines the use of three games for use in the classroom environment about cyber conflict and found that active learning experiences through games lead to more engaged discussion amongst students and improved student ability to articulate security issues.

In conclusion, scenario-related exercises represent a crucial component in the holistic development of cybersecurity and political science students alike. By providing a simulated environment mirroring real-world challenges, these exercises ensure students can develop skills that are difficult to accomplish through traditional lectures and reading (Samaras, Adkins, and White 2022), thus ensuring they are well-prepared for the multifaceted nature of their future roles. The practical application of decision-making, risk management, adaptability, ethical considerations, communication, and strategic planning within scenarios enhances their readiness to contribute effectively to national and global cybersecurity efforts. However, what is important is that any scenario-based or role-playing exercise is methodologically sound in its creation (Biziouras 2013).

In the context of this study, the integration of ChatGPT into scenario-based learning marks a pedagogical innovation that warrants further discussion. Generative AI serves not only as a mechanism to create scenario narratives efficiently, but also as an interactive tool that can simulate dynamic, responsive actors within these scenarios, thus mirroring real-world unpredictability (Ray 2023). This offers new opportunities for learner engagement and formative feedback, allowing students to negotiate with, challenge, or reflect on AI-generated positions, thereby strengthening their analytical and ethical reasoning skills (Li et al. 2025). This supports current discourse that views AI not just as content but as a collaborator in the learning process (Kim, Wang, and Bonk 2025), and highlights its relevance for future cybersecurity education.

Method

Situational context and sampling

The participants in this study were 44 postgraduate students enrolled in an Information Security Management module, which is part of a taught MSc programme delivered by the School of Business, Computing and Social Sciences within a UK university. As the scenario activity was embedded into the normal delivery of the module, participation was naturalistic rather than through formal recruitment. The student cohort represented a diverse group in terms of cultural and academic backgrounds, including both home and international students. The module was timetabled for face-to-face classes over a 12-week period from September to December 2023, where each session was once a week and two hours long. The module content directly relates to the CYBOK knowledge area of 'Risk Management and Governance' (Martin et al. 2021), whilst linking to the Cybersecurity Curricula guidelines knowledge areas of 'organizational security', and 'societal security' since these areas cover topics such as risk management, cyber policy, strategy and planning (Joint Task Force on Cybersecurity Education 2017).

Selecting and drafting the scenarios

The scenario was designed to incorporate a variety of situations that arise in making cybersecurity decisions. It was designed so students would be working in groups, acting as decision makers for a fictional organisation with regard to cybersecurity decisions. Multiple scenarios were created to reflect the diverse nature of events that may take place, ranging from resource planning, business relationships, policies and standards, incident response, and sustainability. Students would work in the same groups each week (groups of approximately 6), and a different scenario would be presented each week for the students to decide for this fictional organisation.

To create the scenarios, Microsoft PowerPoint was used as it is well-known, and does not require new software or purchasing a simulation tool, thus reducing time spent preparing and conducting simulations (Meibauer and Aagaard Nøhr 2018). Furthermore, the large language model of Chat-GPT 3.5[1] was used to aid the creation of the scenarios themselves, as it is free to use, easy to use for people with different levels of technical expertise, and well-suited for producing interactive stories (Adeshola and Praise Adepoju 2023).

Best and Mallinson (2023) considers how technology has evolved throughout the history of the Journal of Political Science Education, and notes how Artificial Intelligence (AI) tools such as ChatGPT are not only applicable for research, but also how they are going to change teaching and learning. Some authors have tried to identify what factors motivate students to use ChatGPT (Foroughi et al. 2023), while others have outlined how AI can be used to create more intricate simulation exercises or session outlines to help students apply the material they are learning (Han et al. 2023). Therefore, AI should be seen more as an opportunity than a threat (Michels 2023), and higher education should consider how tools such as ChatGPT can be integrated into university curriculum (Adeshola and Praise Adepoju 2023). However, given that ChatGPT rose to prominence in November 2022 (Foroughi et al. 2023), there is an evolving corpus of literature detailing how it can and has been used as part of a teaching strategy. Indeed, a literature review study discussing ChatGPT in education considered ninety-three articles and concluded that the keywords 'challenge', 'teaching' and 'knowledge' are not extensively researched (Pradana, Putri Elisa, and Syarifuddin 2023). The authors further suggest that future research could concentrate on examining how ChatGPT could be integrated into teaching practices to achieve an educational goal (Pradana, Putri Elisa, and Syarifuddin 2023). Furthermore, other authors suggested that future studies should focus on how ChatGPT can be used within instructional designs to facilitate learning in higher education (Farrokhnia et al. 2023). Hence, by utilising ChatGPT for the creation of a scenario activity, this study contributes to the knowledge base in this area.

The fictitious scenario name of 'ProtectTech Solutions' was not predefined by the authors but was instead generated by ChatGPT in response to the initial prompt:

'Create a cybersecurity risk management scenario with three decision choices'. The model created this fictional organisation to contextualise the scenario, and this name was subsequently reused in later prompts to maintain narrative consistency. 'ProtectTech Solutions' has no affiliation with any real-world company and was employed purely for illustrative purposes within the generative activity.

ChatGPT was used iteratively and interactively to produce structured decision-making scenarios involving cybersecurity dilemmas. The process involved a sequence of carefully crafted prompts (as shown in Table 1, which includes associated notes for each prompt) beginning with the generation of an initial scenario containing three decision choices. Subsequent prompts refined these scenarios by requesting associated costs, projected cybersecurity and reputation scores, and retrospective narrative descriptions of each decision's outcome. The model's generative capabilities were guided to simulate realistic corporate decision environments, with each prompt building upon prior context to encourage continuity and depth. Multiple iterations were conducted to diversify the scenarios across different themes, including ethical dilemmas and business relationships,

Table 1. ChatGPT prompts and notes.

Prompt	Notes
Create a cybersecurity risk management scenario with three decision choices.	Generates the fictional company of ProtechTech Solutions with a scenario and three choices and outcomes of each choice.
For the above scenario, provide estimated costs for each choice.	Generates costs associated for each choice.
For each of the above scenario choices and outcomes, provide an estimated cybersecurity score and reputation score.	Generates potential implications of each choice with a score for cybersecurity and reputation on a scale of 1–10.
Provide another cybersecurity risk management scenario for ProtectTech Solutions with three decision choices, with costings, and estimated impacts on cyber security score and reputation score.	Generates a comprehensive response based on all requirements identified previously. This is repeated several times to generate a range of scenarios.
Provide another different cybersecurity risk management scenario for ProtectTech Solutions with three decision choices, with costings, and estimated impacts on cybersecurity score and reputation score. Make sure to include an option which has a poor impact on security score and reputation score.	Similar to above, this is used to generate alternative scenarios several times but ensuring that outcomes are more likely to be different.
Provide another different management scenario for ProtectTech Solutions which is an ethical dilemma, with three decision choices, with costings, and estimated impacts on cybersecurity score and reputation score. Make sure all three options lead to a poor impact on security score and reputation score.	Again, similar to above, but ensuring there are some generated scenarios which could all be detrimental.
Provide a paragraph for each outcome for this scenario as if it was after the event happened.	At this stage, text is copied and pasted from previously generated scenarios to generate detailed descriptions of the fictitious outcomes. This is repeated for several scenarios.
Provide another different business relationship scenario (which is detailed) for ProtectTech Solutions with three decision choices, with costings, and estimated impacts on cybersecurity score and reputation score. Make sure to include an option which has a poor impact on security score and reputation score.	Here, ChatGPT has a history of the detail which is required for a scenario. So at this stage, it is asked to generate scenarios for specific topic areas (business relationships in this case). The outcome is a detailed scenario, with detailed costings, impacts on reputation and security score, and a detailed paragraph explaining the outcome for each choice. This is now repeated to generate many scenarios in accordance to what the instructor was looking for.

while deliberately including options that would result in negative outcomes to provoke critical reflection.

While ChatGPT was used as a generative tool to assist in the creation of fictional cybersecurity scenarios, the authors reviewed, refined, and curated all generated content to ensure relevance, coherence, and academic rigour. Hence, some generated scenarios were excluded due to redundancy or unsuitability for the intended student audience.

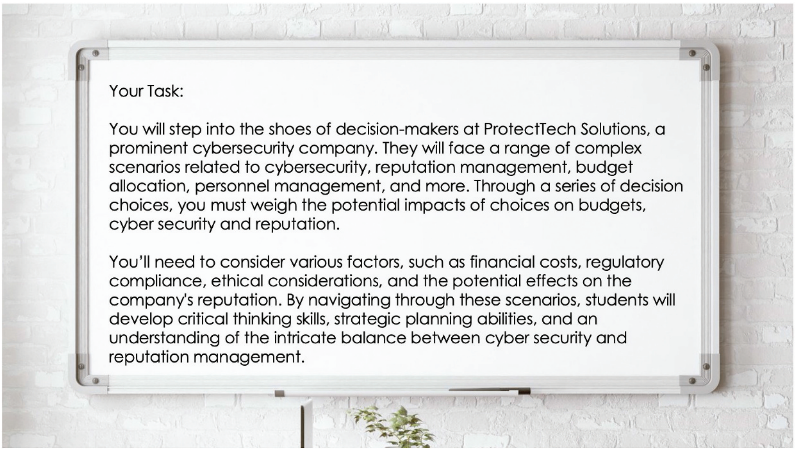
Once suitable scenarios and outcomes were created via ChatGPT 3.5, the content of each scenario could be transferred across into the PowerPoint template to be used in the classroom setting, and edited where necessary in accordance with the language used, metrics provided, etc. With module delivery taking place over twelve weeks, at least twelve scenarios were required to have a scenario each week, but in practice, thirty-six scenarios were created so that there was a resource bank of scenarios that could be used. Although this may seem like a large burden on the designer of the scenario activity, in practice, these 36 scenarios were created and put into a PowerPoint format over one and a half days (approximately 10 hours total). As noted by Michels (2023) and Farrokhnia et al. (2023), this evidences how tools such as ChatGPT can create content in a fraction of the time they would otherwise, even if some modifications were still required. The scenarios were not sequential and so could be 'played' in any order. However, depending on the student groups' metrics (later discussed), how students respond to a scenario would depend on their own current situational context.

It is important to acknowledge that while this study employed ChatGPT 3.5, the AI landscape has evolved significantly since the scenarios were created. More recent large language models such as DeepSeek, GPT-4 (OpenAI), Claude Sonnet 3.5, Gemini (Google), and LLaMA (Meta) have demonstrated enhanced capabilities in reasoning and contextual understanding (Gao et al. 2025). These developments suggest that the use of LLMs in education, particularly for the design of interactive learning tools like scenarios, may become increasingly sophisticated and impactful. Although this paper focuses on the use of GPT-3.5, the pedagogical approach outlined here remains relevant and potentially more powerful when used with contemporary models. Future iterations of this activity may explore and evaluate the impact of these newer models on instructional design and learner engagement.

An example scenario

The following section provides an overview of how the scenarios are designed, illustrated with screenshots from the created scenarios of how to create the scenario slides in PowerPoint. In line with the experience outlined by Meibauer and Aagaard Nøhr (2018) in using PowerPoint-based interactive simulations for undergraduate IR teaching, four different types of slides were used: introduction slides, story slides, choice slides, and end slides. The following example considers a scenario relating to 'business relationships' where a major client requests a new feature to be added to one of the company's products, but it could compromise the security and privacy of users.

Introduction slides present the background to the scenario, and serve as a reminder of the task put to the students. Common to each scenario, the introduction slide (Figure 1), provides a reminder to the students that they are all working for the fictional company of ProtectTech Solutions. ProtectTech Solutions is a cybersecurity company founded in 2015



Your Task:

You will step into the shoes of decision-makers at ProtectTech Solutions, a prominent cybersecurity company. They will face a range of complex scenarios related to cybersecurity, reputation management, budget allocation, personnel management, and more. Through a series of decision choices, you must weigh the potential impacts of choices on budgets, cyber security and reputation.

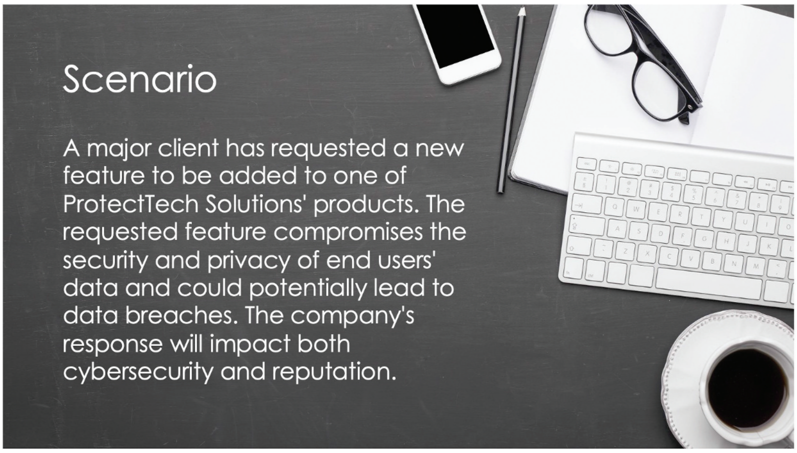
You'll need to consider various factors, such as financial costs, regulatory compliance, ethical considerations, and the potential effects on the company's reputation. By navigating through these scenarios, students will develop critical thinking skills, strategic planning abilities, and an understanding of the intricate balance between cyber security and reputation management.

Figure 1. Introduction slide (common for each scenario).

by a group of seasoned experts in the field. With its headquarters in Cheltenham, ProtectTech has rapidly grown to become a trusted name in providing innovative solutions to safeguard sensitive digital assets for businesses of all sizes. This introduction slide essentially indicates the start of the scenario activity.

Story slides present the narrative for each scenario. They provide students with a background of which choices will need to be made against (Figure 2). Story slides need to be written in such a way that there are multiple choices that could be taken given the narrative presented.

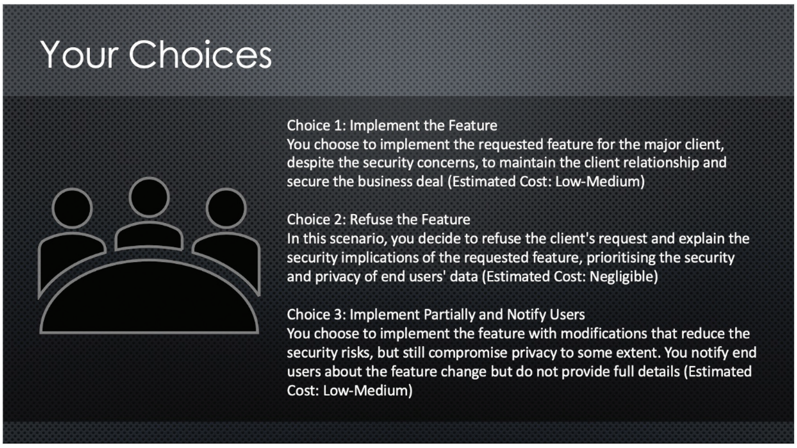
Choice slides are the key component of the scenario activity. They present students with different options to potentially follow, where they can only choose one (Figure 3). Although there could potentially be an unlimited number of choices, a maximum of four has been suggested by authors of similar activities (Meibauer and Aagaard Nøhr 2018). For each scenario used in this study, there were three options for each scenario available



Scenario

A major client has requested a new feature to be added to one of ProtectTech Solutions' products. The requested feature compromises the security and privacy of end users' data and could potentially lead to data breaches. The company's response will impact both cybersecurity and reputation.

Figure 2. Story slide for scenario 5.



Your Choices

Choice 1: Implement the Feature
You choose to implement the requested feature for the major client, despite the security concerns, to maintain the client relationship and secure the business deal (Estimated Cost: Low-Medium)

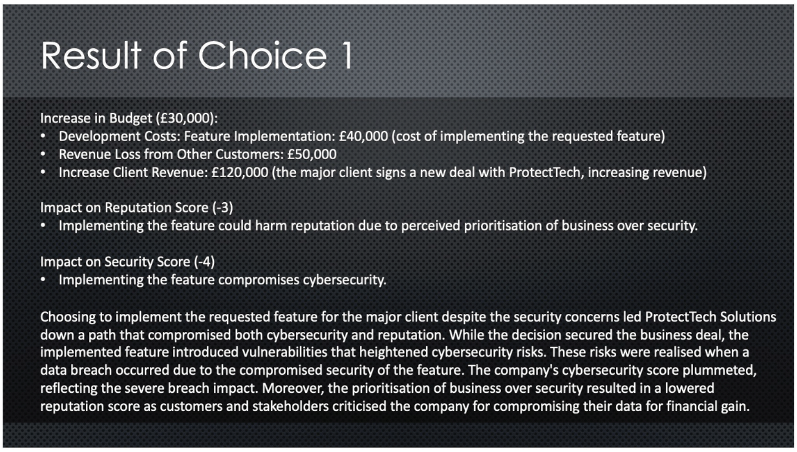
Choice 2: Refuse the Feature
In this scenario, you decide to refuse the client's request and explain the security implications of the requested feature, prioritising the security and privacy of end users' data (Estimated Cost: Negligible)

Choice 3: Implement Partially and Notify Users
You choose to implement the feature with modifications that reduce the security risks, but still compromise privacy to some extent. You notify end users about the feature change but do not provide full details (Estimated Cost: Low-Medium)

Figure 3. Choices slide for scenario 5.

to the students. This was chosen for various reasons. (1) Clarity and simplicity: only having three options makes the scenario clearer and more manageable for learners, allowing for a more focused discussion and in-depth exploration of each choice without being too overwhelmed. (2) Realism: in real-world decision-making, resource constraints may limit the number of feasible options, and decision makers rarely have an exhaustive list. Hence, by focusing on just three choices, learners have to deeply consider the pros and cons of each choice. (3) Time management: classroom time is often limited, and so only having a limited number of choices allows for an efficient use of time in that each learner can thoroughly explore and discuss each available option (Meibauer and Aagaard Nøhr 2018).

The end slides denote the outcome of each choice and address what has happened from each of the previously made choices. The outcomes of the choices can be positive, neutral or negative, and can also depend on the current metrics each student group has. Figure 4 shows the outcome of choosing option one in scenario five. As shown in Figure 4,



Result of Choice 1

Increase in Budget (£30,000):
- Development Costs: Feature Implementation: £40,000 (cost of implementing the requested feature)
- Revenue Loss from Other Customers: £50,000
- Increase Client Revenue: £120,000 (the major client signs a new deal with ProtectTech, increasing revenue)

Impact on Reputation Score (-3)
- Implementing the feature could harm reputation due to perceived prioritisation of business over security.

Impact on Security Score (-4)
- Implementing the feature compromises cybersecurity.

Choosing to implement the requested feature for the major client despite the security concerns led ProtectTech Solutions down a path that compromised both cybersecurity and reputation. While the decision secured the business deal, the implemented feature introduced vulnerabilities that heightened cybersecurity risks. These risks were realised when a data breach occurred due to the compromised security of the feature. The company's cybersecurity score plummeted, reflecting the severe breach impact. Moreover, the prioritisation of business over security resulted in a lowered reputation score as customers and stakeholders criticised the company for compromising their data for financial gain.

Figure 4. End slide for scenario 5 - choice 1.

there are three metrics that are in use for the scenario activity: budget, reputation score, and security score, and each choice will impact each of these three metrics. For the course of study where the scenario tasks were used, student groups began with a budget of £1,000,000, a reputation score of four, and a security score of five. Hence, although student groups were playing 'against' the PowerPoint scenarios like that of (Meibauer and Aagaard Nøhr 2018), as the scenarios progressed, each student group would have their situational context based on these three metrics.

Just three metrics were chosen for the following reasons. (1) Simplicity: By limiting the variables, the scenarios emulate the simplicity often sought in governance structures. Political decisions often involve a multitude of factors, and understanding the core interplay of budget, security, and reputation mirrors the essential components of governance for organisations and government structures alike. (2) Resource allocation: focusing on budget constraints underscores the challenges faced by policymakers in optimally allocating resources to address security concerns and safeguard the reputation of institutions. (3) Interconnectedness of variables: Much like the interconnected nature of political decisions, the chosen variables of budget, security, and reputation are intertwined. (4) Ethical considerations: decision-making often involves ethical considerations. The deliberate inclusion of reputation as a variable prompts learners to grapple with the ethical dimensions of decisions, mirroring the ethical dilemmas faced by political actors.

Given that each student group would have the three metrics, this allowed for some different outcomes to be created depending on each student group's metrics as the scenario activity progressed. For instance, in scenario five, there are two different outcomes for choosing option two depending on a group's reputation score. Refusing the feature request from the major client has a negligible impact, should the student group already have a very high reputation (11+), leading to no impact on security score and reputation, and only £2,000 costs incurred. Whereas if a student groups' reputation score is not as high, then the outcome is that the client relationship is somewhat compromised, leading to a loss of revenue of £100,000, and the reputation score decreasing by one. Ensuring that scenarios had different potential outcomes meant that the variables themselves had more value, and that students would have to consider their own situational context more thoroughly when making decisions. In some cases, the scenarios would end with unsatisfactory outcomes just like that of Meibauer and Aagaard Nøhr (2018), which reflects real-world decision-making. Furthermore, while the scenario choices are not extensively detailed, some authors have described how in a simulation environment, a lack of information for each scenario actually serves as an important lesson about the uncertain nature of decision-making (Garrison, Redd, and Carter 2010).

Using the scenario in class

As indicated above, a scenario is undertaken each class over the period of twelve weeks, and in each class, the scenario occupies approximately 40 minutes of each two-hour session. Throughout each scenario, the lecturer acts as a facilitator as opposed to an instructor. Although there were 44 students enrolled on to the module where this was used, in practice, attendance in class averaged a core group of around 30 students, and they were divided into five groups. Students remained in their groups over the 12 weeks as the scenarios progressed.

The beginning of each scenario involved ensuring students were seated in their student groups, and reminding them of their groups current metrics (budget, security score, and reputation score). Following this, students were introduced to the 'Story' slide for that week's scenario. Here, the scenario is read out aloud to the students while also being shown on the interactive whiteboard. Student groups take a moment to familiarise themselves with the scenario. This whole sequence takes approximately five minutes.

The next step in class is to present the 'Choices' slide for that scenario. This is the heart of the scenario activity. Here, students discuss the options in the groups, to reach a consensus on what option to choose for their groups. Students are encouraged to think of the pros and cons of each option, whilst also considering the potential influence on metrics and their current context. Students are given approximately twenty-five minutes to reach a consensus in their groups. The lecturer facilitates by moving around each group to ascertain progress towards making this consensus and letting students know how much time they have left. Once the twenty-five minutes are finished, the instructor pauses all student group discussions and asks each group to 'lock in' their choice, by getting a representative of each group to provide feedback of their choice to the instructor with some justification of why that option was chosen. The instructor notes the choices chosen on the interactive whiteboard for each group.

Once all groups have their choices 'locked in', the instructor starts to present the 'End' slides for each choice. For each ending, the instructor facilitates some discussion on why that ending was plausible and any important considerations that were made for groups, which chose that option. This part of the scenario activity takes approximately ten minutes. A key consideration for activities such as this is to carefully manage the time spent on discussion and reading out slides (Meibauer and Aagaard Nøhr 2018), and so it is important that the instructor keeps a close watch on the time and is familiar with the scenario being discussed.

Data collection

Although the primary aim of this activity was pedagogical, observational and informal qualitative data were gathered throughout the 12-week period. The module instructor kept reflective field notes during group activities, focusing on how student teams engaged with the decision-making process. Additionally, student outputs and decisions from each scenario were recorded to capture the range of approaches taken. Furthermore, in order to evaluate the scenario, a survey was administered to students in the final week of the module delivery, during which students shared their experiences. It was accessible to students via the virtual learning environment of Moodle, where students could also access module resources. Eight multiple-choice Likert scale questions (mostly 3-point) were asked to students as shown below in Table 2. Here, all questions are normalised to reflect a 3-point scale. Two questions were about knowledge and understanding, two regarding engagement, and four regarding skill development. For each question, students could also add text responses to add any additional comments. Given the population of the student group, a detailed statistical analysis was not conducted, as such a sample would not yield robust or generalisable results. Hence, the additional qualitative aspects were incorporated to explore the nuances of student feedback and to gain insights into their engagement with the scenario-based learning activity.

Table 2. Questions and responses.

What was the impact of the ProtectTech Scenario activity on . . .	Decreased	Neutral	Increased
1) your understanding of course material?	0	0	16
2) your feelings about your ability to do well in the course?	0	0	16
3) your excitement about the course in general?	0	1	15
4) your interest in course material?	1	0	15
5) your decision making skills?	0	0	16
6) your critical thinking skills?	0	1	15
7) your communication skills?	0	3	13
8) your teamwork skills?	0	0	16

Questions 1-4 were adapted from Hendrickson (2021) who investigated different active learning techniques (including simulation) on student excitement, interest and self-efficacy. Hence, these questions were deemed relevant for this study too. Additionally, questions 5–8 followed the same format but focused on four key skills as identified in the earlier literature review; decision making, critical thinking, communication, and teamwork.

The survey itself was not compulsory, and in total sixteen students completed the survey. Prior to completing the survey, students were required to read and agree to the following statement:

> Dear Student, I would like to invite you take part in a study to evaluate the effectiveness of the ProtectTech Scenario Task. The study is voluntary and you will only be included if you provide your permission. Permission will be deemed as granted by filling in this survey. Please note that any participation (or non-participation) will not affect your marks or performance on your course. We do not require personal identifiable information such as your name, student number or email address. Results may be written up into a paper for publication, but as stated, no personal details will be collected and the survey is anonymous. Thank you!

Overall, the data collection approach aligns with a design-based research framework, where iterative classroom practice is used to refine instructional strategies (Fowler and Leonard 2024). No pre-post testing or comparative control group was employed, as the emphasis was on exploratory insight rather than hypothesis testing.

Results and discussion

In this section results of the student survey will be presented, which itself pertains to three main areas; knowledge and confidence, engagement, and skill development. Furthermore, instructor observations will also be presented about the ProtechTech scenario.

Student feedback

Knowledge and confidence

A key objective of the ProtectTech scenario was to allow students to consider course content from the lectures in a more interactive way, with the aim of promoting active learning (Hendrickson 2021; Shanks and Jack Zhang 2023), and hence student understanding of course material. Therefore, students were asked, ‘What was the impact of the

ProtectTech Scenario activity on your understanding of course material?' and 16/16 students answered, 'Increased my understanding'. Student comments included:

> It allowed me understand the dynamics of risk appetite, I am able to integrate it into my assignments and other aspects of cyber security and life. The course gave me a general perspective of organisational options and to realise the opportunity costs.

> It expanded my ability to critic situations and analyse them. In addition to that, it helps me to understand the balance of cybersecurity and business.

This is a very promising result, and supports existing literature indicating how active learning strategies improve student understanding (Fink 2003; Hazari 2005; Maguire, English, and Draper 2019; Yuan et al. 2016).

Self-efficacy, as defined by Bandura (1997) refers to one's belief in their capabilities to successfully complete a task or attain a particular objective. Hence, to ascertain whether the ProtectTech scenario also led to increased self-efficacy, students were asked 'What was the impact of the ProtectTech Scenario Activity on your feelings about your ability to do well in the course?' and six responded, 'somewhat helped my feeling I could do well', and ten responded, 'strongly helped my feeling I could do well'. Therefore, it could be reasoned that the ProtectTech scenario helped improve student self-efficacy. Although this does not directly indicate that students will do well, previous research has indicated that self-efficacy tends to correlate with academic performance (Yokoyama 2019). Additionally, Costa et al. (2015) found that academic achievement is indirectly influenced by student-student interaction, and so this is another reason the scenario is beneficial for student learning.

Engagement: excitement and interest

Students are likely to be more engaged in course content if they feel more connected to the course (Haug, Berns Wright, and Allen Huckabee 2019), and so active learning strategies can be utilised to achieve this aim. Other authors have indicated that lecturers should provide classroom environments that motivate and engage students in the learning process (Costa et al. 2015), and it was the intention of the ProtectTech scenario to do this by increasing course interest and excitement. As indicated by Hendrickson (2021), excitement and interest are similar but distinct concepts, where a student could be interested in the content of the course, but bored with the delivery, while a student may be excited in the course due to its delivery, even if they are not interested in the content. Therefore, students were asked questions on both concepts.

Students were asked 'What was the impact of the ProtectTech Scenario Activity on your excitement about the course in general?' and 15/16 responded that it 'increased my excitement'. One student stated it did not influence excitement positively or negatively. Nevertheless, some students explained how the interactivity and teamwork for the scenarios are what led to increased excitement for the course. For instance, one student commented:

> Discussion with the group and comparing the selection with other groups increases my excitement and always waiting for this activity.

Similarly, another student highlighted how the scenario activity led them to feel motivated to attend class, stating:

> These scenarios kept us motivated and we looked forward to attending the lectures.

Students were also asked, 'What was the impact of the ProtectTech Scenario Activity on your interest in course material?'. One student responded that it decreased their interest, but 15/16 responded that it 'helped my interest'. Therefore, in the case of the ProtectTech scenario, it is evident that the scenario led to increased excitement and interest of the student cohort overall. However, it should be noted that the effectiveness of experiential learning activities such as the ProtectTech scenario depend on student participation (Samaras, Adkins, and White 2022). Although the scenario was partly designed with this focus as a consideration, there is no guarantee another group of students would participate as readily, and so the ProtectTech scenario should be replicated elsewhere to verify its wider effectiveness with regard to enhancing engagement.

Skill development

Van-Laar et al. (2017) conducted a literature review to understand twenty-first century digital-skills, and seven core skills were identified that are important in the workplace; technical, information management, communication, collaboration, creativity, critical thinking and problem solving. Some of these have also been identified in the interdisciplinary arena of cyber security and political science, notably critical thinking, communication, and decision-making (Albert 2021; Grossman and Schortgen 2016, 2016). Hence, understanding whether the ProtectTech scenario led to skill development is important as employers want students who have a blend of technical knowledge and 'soft skills' (Shadbolt 2016). Four questions were therefore asked regarding skill development.

First, students were asked 'What was the impact of the ProtectTech Scenario Activity on your decision making skills?'. Sixteen/16 responded that it 'increased my decision making skills', with one student stating that:

> This activity increased my decision-making skills as we practiced it every week.

Students were also asked, 'What was the impact of the ProtectTech Scenario Activity on your critical thinking skills?'. Fifteen/sixteen students responded that it 'increased my critical thinking skills', while only one student stated it had no effect. Overall, it is clear that critical thinking was improved when considering some of the student comments. As an example, one student explained how the scenario improved their critical thinking ability:

> It improved my critical thinking of false negatives and false positives. To be able to filter that not all good decisions are right to make and not all wrong decisions are best to make.

Students were also asked 'What was the impact of the ProtectTech Scenario Activity on your communication skills?' since communication is required for cybersecurity professionals to articulate complex information (Jones, Siami Namin, and Armstrong 2018), and for political scientists to influence and persuade decision makers and the public (Biziouras 2013). Thirteen/sixteen students responded that the ProtectTech scenario 'increased my communication skills', while three students responded that it had no effect. One student indicated how it was both the student-student interaction, and student-lecturer interaction which led to their improved communication skills:

> As we discuss in groups and discuss with [the lecturer] which increased my communication skills and confidence to participate in class.

Finally, students were asked 'What was the impact of the ProtectTech Scenario Activity on your teamwork skills?'. Sixteen/sixteen responded that it 'increased my ability to work well in a team'. This is certainly very promising and an intended outcome of the scenario task. Most student comments indicated how different aspects of communication were important as part of team work. For instance, the following student comments:

> It made me realise that I am not always right and to see other people perspective which lead to a great impact in the course.

> I strongly agree as I had to give justification for the decision I make and making them agree to it.

In conclusion, this student survey has found that the ProtectTech scenario helps improve student knowledge and confidence, increases engagement, and helps develop important skills required for the fields of cybersecurity and political science.

Instructor observations

Observation 1 – multiple viable choices

For each ProtectTech scenario, there were three options available for students to choose. As shown in Table 3, there was no consensus among student groups overall, with only some instances where each group chose the same option. Hence, this adds credibility to the scenario activity as many of the choices were deemed as viable options by the student cohort. Each group engaged in lots of debate for each option with each group considering the benefits and potential disadvantages of each choice, as well as potential implications on the budget, reputation and cyber security score. In many scenarios, there were conflicting views in the student groups, which fostered further debate and discussion amongst team members. This allowed for further development of communication and teamwork-based skills. Overall, most students contributed to the debates and discussion, and when students were not actively participating, the instructor would encourage them to share their views as the instructor circulate the classroom. As the scenarios resulted in no clear route for students to follow, this meant that each group had different final 'scores' for their budget, reputation and cyber security score, as indicated in Table 4.

Observation 2 – students skills improved

A main observation from the activity was the development of softer skills such as teamwork, communication, and the ability of students to make decisions. As the scenarios and weeks progressed, students appeared to become more conscious of the importance of taking turns to share their views within groups, and also bringing group members into the

Table 3. Student scenario choices each week.

Week	1	2	3	4	5	6	7	8	9	10	11	11	12	12
Scenario	5 (BR)	32 (SP)	35 (RP)	14 (IR)	16 (SU)	4 (BR)	25 (SP)	11 (RP)	33 (SP)	36 (SU)	28 (IR)	17 (RP)	22 (IR)	2 (BR)
Group 1	2	2	1	1	3	3	3	1	1	3	2	2	3	2
Group 2	2	1	2	2	3	3	2	1	1	3	2	3	1	2
Group 3	2	2	1	2	1	3	2	1	2	3	2	2	3	2
Group 4	3	1	2	2	3	3	2	3	2	2	2	2	3	2
Group 5	3	3	2	3	2	3	2	1	1	2	2	1	1	2

Table 4. Final budget, security and reputation scores via student group.

	Budget	Security Score	Reputation Score
Group 1	£ 435,000	14	4
Group 2	£ 505,000	15	9
Group 3	£ 650,000	13	9
Group 4	£ 430,000	12	9
Group 5	£ (135,000)	10	6

discussion who had not contributed yet. Additionally, student groups started to make decisions much faster on what option to choose for each scenario. Consequently, in later weeks, some classes resulted in two scenarios being ‘played’ in one week due to decisions being made so fast. As shown in Table 3, two scenarios were ‘played’ in weeks 11 and 12.

Observation 3 – high student engagement

Overall, students enjoyed the ProtecTech scenario and would often verbally comment that it was one of their favourite aspects of their course. For instance, a mid-module evaluation in week 7 revealed the following comments, when asked what they would like the course to ‘continue’ doing:

> I like his method of teaching and more interesting thing is last part of class thinking about different scenarios and making decisions.
>
> The style of teaching is extremely well, I have studied in Pakistan but never enjoyed this course, but now with [lecturer], the course has become more interesting. Not to forget the scenario based challenge at the end of the class.
>
> I would continue the case studies and the class interactions we have each week. I would love to continue the creative thinking in terms of supporting students achievement in the course.
>
> At the end of lecture the case study scenario is the most valuable and enjoyable part.
>
> Case scenarios are best one and really practical and quite interesting.

In addition to these positive comments on the scenario activity, students would be eager to see the results from the previous week and how their group compared to the others. Similarly, they would actively discuss the decisions in their groups and this included students that were otherwise less engaged in the lecture portion of the class (in terms of contributing ideas, raising of hands etc). Therefore, from an instructor perspective, it was clear how the activity resulted in high student engagement.

Conclusion

This paper has presented ProtechTech Solutions, a ChatGPT-generated scenario-based learning activity designed to foster interdisciplinary competencies at the intersection of cybersecurity and political science. This paper has the following contributions to knowledge and practice.

First, there have been calls for research on the different approaches used for computing and cybersecurity education in terms of pedagogy (Crick et al. 2019; Denny et al. 2019), and this paper directly addresses this in terms of presenting a scenario-based learning activity. This paper supports the assertion that how students in higher education should have opportunities for engaging and applied learning experiences (Chernikova et al. 2020; England, Nagel, and Salter 2020; Omiya and Kadobayashi 2019), as many benefits were obtained. For example, this paper builds upon existing literature that highlights how active learning strategies such as scenarios and simulation can lead to increased student engagement (Mehall 2022; Shanks and Jack Zhang 2023), which for this study, was measured by two variables; interest and engagement. By situating ProtectTech at the intersection of a political, governance, and cybersecurity context, this paper extends prior work by demonstrating how scenario-based learning can also be used to engage with broader civic, regulatory, and communicative dimensions of cyber professional practice, thus building on similar work that focuses explicitly on political analysis (Casey 2024; Khaled et al. 2024).

Second, multiple authors have suggested research should consider how ChatGPT could be integrated into teaching practices to facilitate student learning (Adeshola and Praise Adepoju 2023; Farrokhnia et al. 2023; Pradana, Putri Elisa, and Syarifuddin 2023). This paper directly addresses this research gap and shows how large language models such as ChatGPT can be used from a teaching perspective for the quick and efficient creation of classroom resources. While there is literature detailing examples of practice where tools such as ChatGPT have been utilised, very few detail the prompts required to acquire the results. This is important for instructors who wish to adopt a similar strategy to that of ProtectTech in their own classes. Furthermore, in line with other scholars (Michels 2023), it is believed that these AI tools should not be feared for what potential problems they may bring, but should instead be seen as an opportunity to foster student learning. This work adds nuance to that view by showing how ChatGPT can be pedagogically embedded as a content generator, allowing the creation of resources where students can engage with ethical reasoning, and scenario variability, which is in line with recent evaluations of AI-supported learning environments by Urban et al. (2024) and Zhan and Yan (2025).

Finally, Allison (2023b) found through interviewing computing educators, that developing student soft skills is a key factor for enabling effective student learning. Hence, this paper contributes to knowledge in how scenario-based activities can lead to increased student self-efficacy, and the development of important skills such as decision making, critical thinking, communication, and teamwork. While identified as skills that are required for both cybersecurity specialists and political scientists (Albert 2021; Grossman and Schortgen 2016; Jones, Siami Namin, and Armstrong 2018), these are skills that transcend multiple domains and jobs globally. The ProtectTech scenario was intentionally designed to address this interdisciplinary alignment. The decision-making structure, embedded uncertainties, and requirement for balancing multiple priorities all mirror the complexity of real-world cyber governance, as supported by domain-specific AI integration examples in Santhi and Srinivasan (2024) for cybersecurity, and Ran and Yuyue Zeng (2024) for political science education. Furthermore, the process of creating the ProtectTech scenario could potentially be adapted for other subject areas as well. However, instructors need to be cautious about how their own situational context may influence the effectiveness of such activities, and also what may be most applicable in terms of how to adapt a scenario such as ProtectTech. Hence, future work may explore how different LLMs support or constrain this adaptation process, particularly with respect to disciplinary specificity, output verifiability, and learner experience.

Note

1. https://openai.com/blog/chatgpt.

Disclosure statement

No potential conflict of interest was reported by the author(s).

ORCID

Jordan Allison http://orcid.org/0000-0001-8513-4646

References

Adeshola, Ibrahim, and Adeola Praise Adepoju. 2023. "The Opportunities and Challenges of ChatGPT in Education." *Interactive Learning Environments* 1–14. https://doi.org/10.1080/10494820.2023.2253858.

Albert, Sylvie. 2021. "Applied Critical Thinking in Strategy: Tools and a Simulation Using a Live Case." *Journal of Education for Business* 96 (4): 252–259. https://doi.org/10.1080/08832323.2020.1792395.

Aljaidi, Mohammad, Ayoub Alsarhan, Ghassan Samara, Raed Alazaidah, Sattam Almatarneh, Muhammad Khalid, and Yousef Ali Al-Gumaei. 2022. "NHS Wannacry Ransomware Attack: Technical Explanation of the Vulnerability, Exploitation, and Countermeasures." In *2022 International Engineering Conference on Electrical, Energy, and Artificial Intelligence (EICEEAI)* Zarqa, Jordan, 1–6.

Allison, Jordan. 2023a. "Devising a Cyber Security Management Module Through Integrated Course Design." *Journal of Further and Higher Education* 1–15. https://doi.org/10.1080/0309877X.2023.2250729.

Allison, Jordan. 2023b. "Factors for Enabling Effective Student Learning within English Colleges: The Case of Computing." *Practice: Contemporary Issues in Practitioner Education* 5 (2): 128–143. https://doi.org/10.1080/25783858.2023.2198143.

Asghar, Muhammad Rizwan, and Andrew Luxton-Reilly. 2020. "A Case Study of a Cybersecurity Programme: Curriculum Design, Resource Management, and Reflections." In *Proceedings of the 51st ACM Technical Symposium on Computer Science Education*, New York: 16–22. ACM.

Bandura, Albert. 1997. "Self-Efficacy: The Exercise of Control." In *New York*: W.H. Freeman and Company.

Beerman, Jack, David Berent, Zach Falter, and Suman Bhunia. 2023. "A Review of Colonial Pipeline Ransomware Attack." *In 2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, Bangalore, India: 8–15.

Best, Eric, and Daniel J. Mallinson. 2023. "Quantitative Political Science Education in the Past and Future." *Journal of Political Science Education* 1–13. https://doi.org/10.1080/15512169.2023.2260034.

Biziouras, Nikolaos. 2013. "Bureaucratic Politics and Decision Making Under Uncertainty in a National Security Crisis: Assessing the Effects of International Relations Theory and the Learning Impact of Role-Playing Simulation at the U.S. Naval Academy." *Journal of Political Science Education* 9 (2): 184–196. https://doi.org/10.1080/15512169.2013.770987.

Casey, Daniel. 2024. "ChatGPT in Public Policy Teaching and Assessment: An Examination of Opportunities and Challenges." *Australian Journal of Public Administration*. https://doi.org/10.1111/1467-8500.12647.

Cavelty, Myriam Dunn, and Andreas Wenger. 2020. "Cyber Security Meets Security Politics: Complex Technology, Fragmented Politics, and Networked Science." *Contemporary Security Policy* 41 (1): 5–32. https://doi.org/10.1080/13523260.2019.1678855.

Chernikova, Olga, Nicole Heitzmann, Matthias Stadler, Doris Holzberger, Tina Seidel, and Frank Fischer. 2020. “Simulation-Based Learning in Higher Education: A Meta-Analysis.” *Review of Educational Research* 90 (4): 499–541. https://doi.org/10.3102/0034654320933544.

Costa, Cesário, Ana Paula Cardoso, Margarida Pedroso Lima, Manuela Ferreira, and José Luís Abrantes. 2015. “Pedagogical Interaction and Learning Performance as Determinants of Academic Achievement.” In *Procedia - Social and Behavioral Sciences*. In *5th ICEEPSY International Conference on Education and Educational Psychology* Antalya, Turkey 171, 874–881. https://www.sciencedirect.com/science/article/pii/S1877042815002335.

Crick, Tom, James H. Davenport, Alastair Irons, and Tom Prickett. 2019. “A UK Case Study on Cybersecurity Education and Accreditation.” In *2019 IEEE Frontiers in Education Conference* (FIE), Covington: 1–9. IEEE.

Denny, Paul, Brett A. Becker, Michelle Craig, Greg Wilson, and Piotr Banaszkiewicz. 2019. “Research This! Questions That Computing Educators Most Want Computing Education Researchers to Answer.” In *Proceedings of the 2019 ACM Conference on International Computing Education Research - ICER ’19*, New York, NY, USA: 259–267. ACM Press.

Egloff, Florian J. 2020. “Contested Public Attributions of Cyber Incidents and the Role of Academia.” *Contemporary Security Policy* 41 (1): 55–81. https://doi.org/10.1080/13523260.2019.1677324.

England, Trevor K., Gregory L. Nagel, and Sean P. Salter. 2020. “Using Collaborative Learning to Develop Students’ Soft Skills.” *Journal of Education for Business* 95 (2): 106–114. https://doi.org/10.1080/08832323.2019.1599797.

Farrokhnia, Mohammadreza, Seyyed Kazem Banihashem, Omid Noroozi, and Arjen Wals. 2023. “A SWOT Analysis of ChatGPT: Implications for Educational Practice and Research.” *Innovations in Education and Teaching International* 1–15. https://doi.org/10.1080/14703297.2023.2195846.

Fidler, David P. 2011. “Was Stuxnet an Act of War? Decoding a Cyberattack.” *IEEE Security & Privacy Magazine* 9 (4): 56–59. https://doi.org/10.1109/MSP.2011.96.

Fink, Dee. 2003. *A Self-Directed Guide to Designing Courses for Significant Learning*. San Francisco: Jossey Bass.

Foroughi, Behzad, Madugoda Gunaratnege Senali, Mohammad Iranmanesh, Ahmad Khanfar, Morteza Ghobakhloo, Nagaletchimee Annamalai, and Bita Naghmeh-Abbaspour. 2023. “Determinants of Intention to Use ChatGPT for Educational Purposes: Findings from PLS-SEM and fsQCA.” *International Journal of Human–Computer Interaction* 1–20. https://doi.org/10.1080/10447318.2023.2226495.

Fowler, Samuel, and Simon N Leonard. 2024. “Using Design Based Research to Shift Perspectives: A Model for Sustainable Professional Development for the Innovative Use of Digital Tools.” *Professional Development in Education* 50 (1): 192–204. https://doi.org/10.1080/19415257.2021.1955732.

Gao, Tianchen, Jiashun Jin, Zheng Tracy Ke, and Gabriel Moryoussef. 2025. “A Comparison of DeepSeek and Other LLMs.” *ArXiv Preprint ArXiv: 2502.03688* doi:https://doi.org/10.48550/arXiv.2502.03688.

Garrison, Jean A., Steven B. Redd, and Ralph G. Carter. 2010. “Energy Security Under Conditions of Uncertainty: Simulating a Comparative Bureaucratic Politics Approach.” *Journal of Political Science Education* 6 (1): 19–48. https://doi.org/10.1080/15512160903467653.

Grossman, Michael, and Francis Schortgen. 2016. “Building a National Security Program at a Small School: Identifying Opportunities and Overcoming Challenges.” *Journal of Political Science Education* 12 (3): 318–334. https://doi.org/10.1080/15512169.2015.1103653.

Hajny, Jan, Sara Ricci, Edmundas Piesarskas, Olivier Levillain, Letterio Galletta, and Rocco De Nicola. 2021. “Framework, Tools and Good Practices for Cybersecurity Curricula.” *IEEE Access* 9:94723–94747. https://doi.org/10.1109/ACCESS.2021.3093952.

Han, Zhiyong, Fortunato Battaglia, Abinav Udaiyar, Allen Fooks, and Stanley R. Terlecky. 2023. “An Explorative Assessment of ChatGPT as an Aid in Medical Education: Use it with Caution.” *Medical Teacher* 1–8. PMID: 37862566, https://doi.org/10.1080/0142159X.2023.2271159.

Haug, James C, Linda Berns Wright, and W. Allen Huckabee. 2019. “Undergraduate Business Students’ Perceptions About Engagement.” *Journal of Education for Business* 94 (2): 81–91. https://doi.org/10.1080/08832323.2018.1504738.

Hazari, Sunil. 2005. "Instructional Strategies for a Graduate Level Information Security Management Course." In *InfoSecCD Conference'04* Kennesaw Georgia, 71–75. ACM.

Hendrickson, Petra. 2021. "Effect of Active Learning Techniques on Student Excitement, Interest, and Self-Efficacy." *Journal of Political Science Education* 17 (2): 311–325. https://doi.org/10.1080/15512169.2019.1629946.

Herr, Trey, Arthur P. B. Laudrain, and Max Smeets. 2021. "Mapping the Known Unknowns of Cybersecurity Education: A Review of Syllabi on Cyber Conflict and Security." *Journal of Political Science Education* 17 (sup1): 503–519. https://doi.org/10.1080/15512169.2020.1729166.

Hoke, Candice. 2010. "Internet Voting: Structural Governance Principles for Election Cyber Security in Democratic Nations." In *Proceedings of the 2010 Workshop on Governance of Technology, Information and Policies, GTIP '10*, New York, NY, USA: 61–70. Association for Computing Machinery. https://doi.org/10.1145/1920320.1920329.

Joint Task Force on Cybersecurity Education. 2017. *Cybersecurity Curricula 2017: Curriculum Guidelines for Post-secondary Degree Programs in Cybersecurity*. New York: Association for Computing Machinery.

Jones, Keith S., Akbar Siami Namin, and Miriam E. Armstrong. 2018. "The Core Cyber-Defense Knowledge, Skills, and Abilities That Cybersecurity Students Should Learn in School: Results from Interviews with Cybersecurity Professionals." *ACM Transactions on Computing Education* 18 (3): 12. https://doi.org/10.1145/3152893.

Khaled, AL-Mhasneh, AL-Arqan Abedalrahim Rashed Alrasheed, Juwaireya Fares, Munays Alqahtani, and Amal Salman. 2024. "The Role of Artificial Intelligence in Political Analysis and Decision Aid: "Chat GPT Application" as a Model." In *2024 International Conference on Decision Aid Sciences and Applications (DASA)*, Manama, Bahrain, 1–4. IEEE.

Kim, Paul, Wilson Wang, and Curtis J Bonk. 2025. "Generative AI as a Coach to Help Students Enhance Proficiency in Question Formulation." *Journal of Educational Computing Research* 63 (3): 1–22. https://doi.org/10.1177/07356331251314222.

Li, Pin-Hui, Hsin-Yu Lee, Chia-Ju Lin, Wei-Sheng Wang, and Yueh-Min Huang. 2025. "Inquirygpt: Augmenting ChatGPT for Enhancing Inquiry-Based Learning in STEM Education." *Journal of Educational Computing Research* 62 (8): 2157–2186. https://doi.org/10.1177/07356331241289824.

Maguire, Joseph, Rosanne English, and Steve Draper. 2019. "Data Protection and Privacy Regulations as an Inter-Active-Constructive Practice." *Proceedings of the 3rd Conference on Computing Education Practice*, Durham, United Kingdom: 1–4. ACM. jan.

Martin, Andrew, Awais Rashid, Howard Chivers, Steve Schneider, Emil Lupu, and George Danezis. 2021. *Introduction to CyBOK Knowledge Areas*. Technical Report. Bristol: Bristol Cyber Security Group.

Masood, Rahat, Ume Ghazia, and Zahid Anwar. 2011. "SWAM: Stuxnet Worm Analysis in Metasploit." *2011 Frontiers of Information Technology*: 142–147.

Mehall, Scott. 2022. "Comparing In-Class Scenario-Based Learning to Scenario-Based eLearning Through an Interactive, Self-Paced Case Study." *Journal of Education for Business* 97 (5): 305–311. https://doi.org/10.1080/08832323.2021.1943294.

Meibauer, Gustav, and Andreas Aagaard Nøhr. 2018. "Teaching Experience: How to Make and Use PowerPoint-Based Interactive Simulations for Undergraduate IR Teaching." *Journal of Political Science Education* 14 (1): 42–62. https://doi.org/10.1080/15512169.2017.1377083.

Metcalf, Leigh. 2021. "Editorial on the Special Issue on Election Security." *Digital Threats* 2 (4): 1–1. https://doi.org/10.1145/3471534.

Michels, Steven. 2023. "Teaching (With) Artificial Intelligence: The Next Twenty Years." *Journal of Political Science Education* 1–12. https://doi.org/10.1080/15512169.2023.2266848.

Naugle, Asmeret Bier, Michael L. Bernard, and Itamara Lochard. 2016. "Simulating Political and Attack Dynamics of the 2007 Estonian Cyber Attacks." *Proceedings of the 2016 Winter Simulation Conference, WSC*, Washington, DC, USA'16, 3500–3509. IEEE Press.

Omiya, Tan, and Youki Kadobayashi. 2019. "Secu-One: A Proposal of Cyber Security Exercise Tool for Improving Security Management Skill." In *Proceedings of the 2019 7th International Conference on Information and Education Technology - ICIET 2019*, New York: 259–268. ACM.

Parrish, Allen, John Impagliazzo, Rajendra K. Raj, Henrique Santos, Muhammad Rizwan Asghar, Audun Jøsang, Teresa Pereira, and Eliana Stavrou. 2018. "Global Perspectives on Cybersecurity Education for 2030: A Case for a Meta-Discipline." *Proceedings Companion of the 23rd Annual ACM Conference on Innovation and Technology in Computer Science Education*, New York: 36–54. ACM. jul.

Pope, Amy E. 2018. "Cyber-Securing Our Elections." *Journal of Cyber Policy* 3 (1): 24–38. https://doi.org/10.1080/23738871.2018.1473887.

Pradana, Mahir, Hanifah Putri Elisa, and Syarifuddin Syarifuddin. 2023. "Discussing ChatGPT in Education: A Literature Review and Bibliometric Analysis." *Cogent Education* 10 (2): 2243134. https://doi.org/10.1080/2331186X.2023.2243134.

Praprotnik, Gorazd, Teodora Ivanuša, and Iztok Podbregar. 2013. "EWar - Reality of Future Wars." *Proceedings of the 2013 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM '13*, New York, NY, USA: 1068–1072. Association for Computing Machinery. https://doi.org/10.1145/2492517.2500321.

Qian, Xuming. 2019. "Cyberspace Security and U.S.-China Relations." *Proceedings of the 2019 International Conference on Artificial Intelligence and Computer Science, AICS 2019*, New York, NY, USA: 709–712. Association for Computing Machinery. https://doi.org/10.1145/3349341.3349495 .

Ran, Xiaoping, and Yuyue Zeng. 2024. "Research on the Scenario Application of Generative Artificial Intelligence in Ideological and Political Education of Colleges and Universities." *Proceedings of the 2024 International Conference on Big Data and Digital Management*, Shanghai, China, 454–459.

Ray, Partha Pratim. 2023. "ChatGPT: A Comprehensive Review on Background, Applications, Key Challenges, Bias, Ethics, Limitations and Future Scope." *Internet of Things and Cyber-Physical Systems* 3:121–154. https://doi.org/10.1016/j.iotcps.2023.04.003.

Ricci, Sara, Vladimir Janout, Simon Parker, Jan Jerabek, Jan Hajny, Argyro Chatzopoulou, and Remi Badonnel. 2021. "PESTLE Analysis of Cybersecurity Education." The 16th International Conference on Availability, Reliability and Security, New York: 1–8. ACM. aug.

Samaras, Steven A., Cheryl L. Adkins, and Charles D. White. 2022. "Developing Critical Thinking Skills: Simulations vs. Cases." *Journal of Education for Business* 97 (4): 270–276. https://doi.org/10.1080/08832323.2021.1932703.

Santhi, Thulasi M, and K. Srinivasan. 2024. "Chat-GPT Based Learning Platform for Creation of Different Attack Model Signatures and Development of Defense Algorithm for Cyberattack Detection. IEEE Transactions on Learning Technologies, 17, pp: 1829–1842. doi:10.1109/TLT.2024.3417252.

Schoettmer, Patrick L. 2023. "Survival!: A Portable Simulation That Encourages Failure." *Journal of Political Science Education* 19 (3): 496–510. https://doi.org/10.1080/15512169.2023.2167208.

Shadbolt, Nigel. 2016. *Shadbolt Review of Computer Sciences Degree Accreditation and Graduate Employability*. London: Department for Business, Innovation and Skills.

Shanks, Spencer, and Jiakun Jack Zhang. 2023. "Disentangling Perception and Performance: A Natural Experiment on Student Engagement and Learning in Simulations." *Journal of Political Science Education* 1–26. https://doi.org/10.1080/15512169.2023.2245511.

Stevens, Clare. 2020. "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet." *Contemporary Security Policy* 41 (1): 129–152. https://doi.org/10.1080/13523260.2019.1675258.

Toapanta, Segundo Moisés T., Luis Briones Peñafiel, and Luis Enrique Mafla Gallegos. 2020. "Prototype to Mitigate the Risks of the Integrity of Cyberattack Information in Electoral Processes in Latin America." In *Proceedings of the 2019 2nd International Conference on Education Technology Management*. ICETM '19, New York, NY, USA: 111–118. Association for Computing Machinery. https://doi.org/10.1145/3375900.3375915.

Urban, Marek, Filip Děchtěrenko, Jiří Lukavskỳ, Veronika Hrabalová, Filip Svacha, Cyril Brom, and Kamila Urban. 2024. "ChatGPT Improves Creative Problem-Solving Performance in University Students: An Experimental Study." *Computers and Education* 215:105031. https://doi.org/10.1016/j.compedu.2024.105031.

Van-Laar, Ester, Alexander J.A.M. Van-Deursen, Jan A.G.M. Van-Dijk, and Jos De-Haan. 2017. "The Relation Between 21st-Century Skills and Digital Skills: A Systematic Literature Review." *Computers in Human Behavior* 72:577–588. https://doi.org/10.1016/j.chb.2017.03.010.

Whyte, Christopher. 2021. “Using Mini-Games to Teach Cyber Issues to Social Science Students.” *Journal of Political Science Education* 17 (sup1): 215–225. https://doi.org/10.1080/15512169.2020.1737537.

Yang, Tzu-Chi, Yi-Chuan Hsu, and Jiun-Yu Wu. 2025. “The Effectiveness of ChatGPT in Assisting High School Students in Programming Learning: Evidence from a Quasi-Experimental Research.” *Interactive Learning Environments* 33 (6): 1–18. https://doi.org/10.1080/10494820.2025.2450659.

Yokoyama, Satoru. 2019. “Academic Self-Efficacy and Academic Performance in Online Learning: A Mini Review.” *Frontiers in Psychology* 9. https://www.frontiersin.org/articles/10.3389/fpsyg.2018.02794.

Yuan, Xiaohong, Wu He, Li Yang, and Lindsay Simpkins. 2016. “Teaching Security Management for Mobile Devices.” *Proceedings of the 17th Annual Conference on Information Technology Education*, New York: 14–19. ACM. sep.

Zhan, Ying, and Zi Yan. 2025. “Students’ Engagement with ChatGPT Feedback: Implications for Student Feedback Literacy in the Context of Generative Artificial Intelligence.” *Assessment and Evaluation in Higher Education*: 1–14. https://doi.org/10.1080/02602938.2025.2471821.