CAP: Patching the Human Vulnerability

Thaddeus Eze and Neil Hawker

Computer Science Department, University of Chester, England
t.eze@chester.ac.uk n.hawker@chester.ac.uk

Abstract. Cyber threats to organisations across all industries are increasing in both volume and complexity, leading to significant, and sometimes severe, consequences. The common weakest link in organisations security is the human vulnerability. The sudden popularity of remote-working due to the Covid-19 pandemic opened organisations and their employees up to more risks, particularly as many workers believe that they are more distracted when at home. Existing cyber training using a 'one-size-fits-all' approach has been proven inefficient/ineffective and the need for a more fit-for-purpose training is required. When it comes to cyber training, we know that there is no single-training-fits-all solution – people have different technical skills, different prior knowledge and experience, are in different roles, exposed to different security risks, and require knowledge that is relevant to what they do. This study makes a case for tailored role-based cybersecurity training suitable for awareness within organisations across multiple industries. The study explores the strengths and weaknesses of existing cyber training and literature to make recommendations on efficient awareness and training programme strategies. The study carries out knowledge and task analysis of job roles to create profiles of skills and knowledge they require. These are grouped by topic and level to form scenario-based multiple-choice questions which are mapped to create a Cyber Awareness Platform (CAP). A CAP prototype is introduced as a flexible web-based system allowing users to assess their prior knowledge and skills personalised to their role. Knowledge gaps and training needs are identified, and recommendations are tailored to the individual. Initial analysis of CAP shows promising results, indicating that such role-sensitive solution would be highly beneficial to users. This offers further development opportunities in producing an all-in-one cyber assessment and training platform.

Keywords: Cyber Awareness Platform, Cybersecurity Awareness, Role-based Training, Human Vulnerability, Tailored Cybersecurity, Task Analysis.

1 Introduction

Businesses have been able to benefit significantly from developments in technology that allows them to interact with their customers, suppliers, and other businesses in the digital world. No longer are trading hours restricted to those of a physical store presence. Businesses can trade 24/7 using e-commerce, mobile apps, smart home digital assistants, and through social media channels. However, as these technologies are adopted, they bring new security risks and challenges, leading to more attack surfaces.

Bad actors take advantage of security vulnerabilities to attack business information systems which can lead to data breaches. Confidential data such as employees' logins, company secrets, and customer personal data are then at risk of being leaked, resulting in major reputational damage and serious ramifications that can be hard to recover from. A study by VMware Carbon Black [1] reported 70% of respondents had suffered from damages to their brand image following a data breach. Rankin [2] puts the average cost of a data breach at $141 for each record stolen while IBM [3] explains that an average breach involves 25,575 records. According to [3], the average time to identify and contain a breach is 279 days and the average cost of a data breach rose 12% between 2015 and 2020, costing about $3.92 million to correct.

The UK's Information Commissioners Office fined the University of Greenwich £120,000 in 2018 after multiple cyber-attacks on a legacy microsite resulted in around 20,000 people's personal data being breached [4]. The site that was to facilitate a conference in 2004 was not shutdown or maintained. This meant it was susceptible to SQL injection attacks in 2013 which led to further attacks in 2016 [4]. The 2017 WannaCry ransomware attack on the UK's National Health Service (NHS) was partly possible due to a significant number of machines within the NHS, at the time, running on older unpatched versions of Windows. In 2018, British Airways (BA) revealed it had been victim to a data breach leaking 380,000 customers personal and payment details [6]. The rogue code, a web-based card skimmer, used by the attackers sent personal and credit card information silently to a disguised, but legitimate looking domain '*baways.com*' once customers press the submit button. In 2015, a clinic staff in London accidentally leaked sensitive information of patients by using Cc (Copy) instead of Bcc (Blind Copy) in an email[1]. These, and most successful breaches, are due to human errors.

Human error is the weakest security link and continues to be the common reason for successful cyber-attacks and data breaches [7-8]. A study by Hancock [9] to understand the impacts of human mistakes and vulnerabilities on cybersecurity found that 88% of data breaches are caused by human error. Common human errors causing successful cyber-attacks include system misconfiguration, poor patch management, use of default usernames/passwords and easily guessable passwords, loss of mobile devices, and disclosure of controlled information via email [7]. A major rise in cyber-attacks, targeting home workers since the Covid-19 pandemic, involving malicious emails attempting to steal employee credentials have been reported [10]. These phishing attempts involved tricking employees to use fake sign-in pages for systems they would regularly use. Employee's corporate accounts for VPNs and video conferencing accounts such as Zoom were frequently targeted. It is then evident that reducing the level of human errors will significantly improve cyber security posture. The best patch for human vulnerability has always been training, awareness, and education. With well-trained employees, organisations can be more prepared and protected from cyber-attacks. However, training needs to be fit-for-purpose.

The traditional cybersecurity training approaches are mostly ineffective in changing employees' behaviours. These behaviours have proven the human as the weakest link in cybersecurity. A usual practice, within organisations, is to have a generic training

[1] https://bit.ly/3qaQw83

programme for everyone. So, if an organisation wishes to sign up for staff training, they choose a provider or a training course and lump everyone into it. However, when it comes to cyber training, we know that there is no *single-training-fits-all* solution – people have different technical skills, different prior knowledge and experience, are in different roles, exposed to different security risks (some more complex than others), require knowledge that is relevant to what they do etc.

An efficient solution would be a role-based tailored training approach that involves a generic classification of roles as well as a finer-grained classification that considers the individual's personal prior knowledge in addition to their role. There is an increase in recent studies recommending tailored training as against generic '*off the shelf*' packages [7-8, 11]. Although role-based/tailored training is not new, it is not sufficient to consider the individual's role in determining their training requirement without also considering their prior knowledge. So, the question is whether we can come up with a tailored training system that appreciates people's prior knowledge and current role. A starting point is to design a system that can correctly determine one's relevant cyber-related knowledge and be able to recommend required role-based training. This will involve task analysis to be able to understand different roles in order to capture what is relevant to them in terms of cyber knowledge. This project attempts to answer the question; '*What is an appropriate cybersecurity training and/or body of knowledge for the particular individual*'? This involves thorough overview of existing approaches and articulation of a widely accepted solution. It is expected that the intended product, the CAP, would help companies organise efficient and fit-for-purpose cyber training.

With regards to training, the focus of our proposed solution is not on mode of delivery. Yes, nature/mode of delivery is an important aspect to consider as well as the content itself. However, the question that needs to be answered first is '*what (in terms of content) constitute an effective and efficient training for the individual (emphasis on personalised, role-based training)*'? This will need to explore/address a number of issues – task analysis, knowledge analysis, existing or new cybersecurity body of knowledge, understanding the individual's position on the knowledge spectrum etc. So, the proposed role-based tailored training is not limited to a generic classification of known role groups. It takes a finer-grained approach of determining role grouping and the consideration of prior and required knowledge within those groups.

2 Literature Review

The question of terminology needs to be addressed first. Cybersecurity awareness, training, and education all involve some level of learning that leads to changes in user behavior. Although they are sometimes used interchangeably, they do differ in meaning. Awareness establishes a generic foundation of security understanding and deals with security related issues that all users, regardless of job role, must be aware of. Training deals with teaching the user the dos and don'ts, while performing their tasks, in order to meet specific security requirements. Education is a more formal arrangement of pursuing a wider knowledge and usually offered by a third party. See [12] for more details. In the context of this paper, cyber awareness/training is where a person has both

the knowledge and the understanding of the importance of information security to protect themselves and/or the organisation they work for from cyber-crime/attack [13-14].

There are several existing cybersecurity awareness and training resources available, including research that identify recommendations for creating successful cyber training. While these are interesting materials, most are about modes or methods of training delivery and not about how to determine what training, in terms of content, is needed.

2.1 Existing Cyber Security Awareness and Training

The UK National Cyber Security Centre (NCSC)'s study [15] to understand training issues with small to medium sized enterprises (SMEs) highlighted key issues of organisations struggling to explain why cybersecurity is important and explained technical aspects that are relevant to employees. They produced two set of resource materials for users, depending on their technical knowledge. The '*Top Tips for Staff*' training package, covering defending against phishing, using strong passwords, securing devices, and reporting incidents with the premise '*if in doubt, call it out*' is aimed at those staff who have little to no technical knowledge. The '*10 Steps to Cyber Security*' guidance [11] helps security and technical staff within organisations manage their cybersecurity risks. These materials can be used as base layer of core cybersecurity skills required for training that are applicable to all employees within an organisation. NCSC [11], as well as [7-8], recommend, and we agree, tailoring cybersecurity training to the needs of the organisation rather than having a generic *off-the-shelf* training package.

Regner *et al*. [8] proposed their 'Cybersecurity Awareness TRAining Model (CATRAM)' as a replacement for traditional cybersecurity training that have become ineffective in changing employee's behaviour. This is asserted from the fact that human error and actions continue to happen despite organisations having strong security controls in place. According to [8], CATRAM addresses the deficiencies in existing cyber awareness and training available. The model targets different levels of role within an organisation such as board level, executives, managers, and IT specialists. Each level has their own part to play in promoting and ensuring a consistent cyber aware approach to threats. Axelos [16] supports cyber specific training, tailored to employee roles that takes place on a regular basis. The CATRAM model is designed to be adapted and used across multiple industries and audiences, making it more flexible and effective than traditional cyber training programs [8]. The role-based tailored training proposed by [8] follows a generic classification of roles. Whereas this is an interesting solution, a more effective approach would consider the individual's personal prior knowledge in addition to their role. This new approach would start with role grouping and then move on to consider prior knowledge within those groups.

He and Zhang [7], in their study, 'Enterprise cybersecurity training and awareness programs: Recommendations for success', put forward a number of recommendations for a successful cybersecurity training. Two of the recommendations include *Personalisation* – using examples that help employees relate to the training and also instill the behaviour that cybersecurity risks are not just at work but at home too, and *Relevancy* – providing training that is tailored to roles and responsibilities.

The case can be made that tailored training, whether in delivery or determining need, is efficient and yields better result in the long-term. McCormac *et al*. [17] state that there is potential value in tailoring cybersecurity training to a person's personality and learning style, which could maximise participants learning outcomes. Pattinson *et al*. [18] found that matching an individual's learning style to appropriate training improves the participants information security awareness (ISA) and that an individual's ISA score did not increase significantly when training regularity was increased, suggesting that an organisation may not need to increase their training budget but instead tailor training to the individual.

2.2 Related Studies

Shinoda *et al*. [19] propose their cybersecurity training framework CyTrONE, which uses classical training paradigm of scenario and topic-based questions along with practical exercises. This is an important means for assessing a person's competencies and weaknesses. Whilst [19] involves the creation of a practical training environment, which is beyond the scope for this study, it is still useful as it also deals with cybersecurity training content generation and environment setup tasks which is a focus and aspect considered by CAP. Lessons from CyTrONE will feed into CAP future research.

A study [20] for developing cyber education and training for the UK police forces focused on various roles within a police force and involved establishing responsibilities and role-based knowledge and skills profiles within that force. A web-based prototype tool was created to allow employees assess their individual cybercrime training needs [20]. The research links into this study as it involves assessing employee's cyber awareness and training needs whilst also considering their role and prior knowledge.

Oyinloye [21] also carried out a study to develop an application to determine an understanding of a user's cybersecurity awareness and make suggestions based on these outcomes. [21] is useful to draw lessons from as it found participants in awareness tests who scored high overall had weaknesses in other areas such as viruses and malware, so it is important to tailor training recommendations to individual responses.

Overall, the studies and works discussed in this review highlighted the need for a tailored cyber training solution over one-size-fits-all approaches for organisations. One key finding is that whilst there are examples of tailored training [8, 22], there is still a gap for taking employees existing knowledge into consideration as part of the tailored training. Skills frameworks, e.g., CIISec [23] and SFIA [24], can be used to inform this study's skills and roles mapping design. This is discussed further in the next section.

2.3 Assessing and Measuring Skills

Assessing a person's prior cybersecurity related knowledge and using that information to determine their training need is an important aspect of CAP. The ability to assess and measure an employee's skills is crucial to understanding their specific training needs. The Chartered Institute of Information Security (CIISec) Skills Framework [23] provides basis of what knowledge and skills are expected for 11 security disciplines – from

level 1 (basic knowledge) to 6 (expert/lead practitioner) in each discipline. Fig. 1 shows sections of the framework along with associated security disciplines.

Fig. 1. CIISec framework skills areas and security disciplines [23].

The CIISec skills, knowledge, and role frameworks are a strong basis for developing assessment questions to assess a person's knowledge against a section. An example for a software developer could be testing section C level 3 (*C3 – Secure Development*) to see which level that particular employee meets. It would then be possible to identify appropriate training on a level-by-level basis for employees by role [23]. Watkins *et al.* [25] explain the methods available for carrying out needs assessments to make decisions. On a basic principle, the first steps to a need's assessment are to identify the gaps between the current state and desired state. In this study, it is the gaps in an employee's cyber awareness knowledge. Determining the employee's needs can be done by skills mapping to a framework such as [23]. Where the outcome is a lower skill level than desired, interventions can be put in place to highlight these and refer to suitable training.

Fig. 2. SFIA diagram showing the elements that make up the competency framework [24].

Skills Framework for the Information Age (SFIA) is a not-for-profit organisation and model for managing skills and competencies for those working in IT and other digital disciplines. The elements that make up the framework are shown in Fig. 2. SFIA [26] state that everybody has information security responsibilities and should make it

part of their day-to-day working. Each SFIA level increases in information security responsibilities as shown in Table 1. SFIA skills can be mapped to other frameworks such as NICE (National Initiative for Cybersecurity Education) work roles [27]. The framework is comprised of 7 high-level categories of common cybersecurity areas, 33 distinct areas of cybersecurity work and importantly 52 work roles. The work roles are in detailed groupings of what is expected in those roles made up of specific knowledge, skills, and abilities to perform tasks within that role [28]. Whereas the NICE framework's focus is cybersecurity roles, the SFIA framework is applicable to wider roles that interact with IT [24].

Table 1. SFIA Information security attributes in levels of responsibility [26].

SFIA Level	Information security attributes and responsibilities
1 Follow	Understands and applies basic personal security practice
2 Assist	Is fully aware of and complies with essential organisational security practices expected of the individual
3 Apply	Understands how own role impacts security and demonstrates routine security practice and knowledge required for own work
4 Enable	Fully understands the importance of security to own work and the operation of the organisation. Seeks specialist security knowledge or advice when required to support own work or work of immediate colleagues
5 Ensure, Advise	Proactively ensures security is appropriately addressed within their area by self and others. Engages or works with security specialists as necessary. Contributes to the security culture of the organisation
6 Initiate, Influence	Takes a leading role in promoting security throughout own area of responsibilities and collectively in the organisations
7 Set Strategy, Inspire, Mobilise	Champions security within own area of work

These frameworks are instrumental in the classification of role-holder's knowledge and design of knowledge assessment for the Cyber Awareness Platform (CAP).

3 CAP Design

CAP is a tailored framework that helps us understand the cybersecurity need of an individual and identify a suitable training for that individual. The system can assess a person's cybersecurity knowledge and identify knowledge gaps whilst considering their role-profile and existing skills. Fig. 3 shows the different components that make up the CAP framework. To efficiently recommend an appropriate training, the system considers two important aspects – *Knowledge* and *Task*. Knowledge Analysis (KA) establishes a mapping of recognised body of knowledge against which any claim of cybersecurity knowledge can be tested. This can feed from the CyBOK[2] knowledge areas [29] and/or any existing cybersecurity body of knowledge like the CIISec and SFIA frameworks discussed in Section 2. The vPK component identifies the user's

[2] https://www.cybok.org/

cybersecurity knowledge with reference to the body of knowledge expressed in KA. KA's knowledge base provides a basis for developing assessment questions from which to assess a person's knowledge against different areas. This can test generic or specific knowledge, depending on implementation choice.

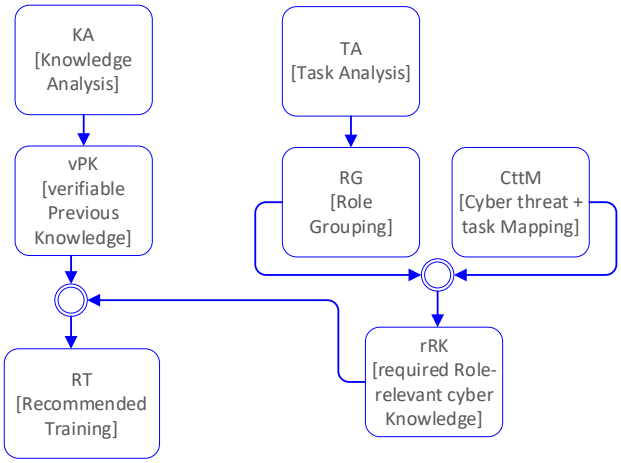

Fig. 3. CAP Framework.

Task Analysis (TA) determines the tasks employees (users) are expected to undertake by role. The guide to task analysis in [30] is a good reference for conducting TA. The result here is an understanding of the relevant activities or tasks performed by a role which will help in determining the kind of cybersecurity risks the role faces. Job descriptions and person specifications are good sources of information here. This means that roles are coded into the system, making CAP adaptable, and for that to happen, roles need to be grouped. RG deals with classification of identified roles into groups of common themes, from cybersecurity viewpoint. These could be high-level or detailed groupings of roles with similar or overlapping requirements and tasks. This makes it easier to understand and define a set of cybersecurity threats associated to those task groups (CttM). So, the CttM component establishes the common cybersecurity threats associated to roles. Although there are generic security threats (e.g., human error), there are also threats that are unique to certain job roles (e.g., whaling). The outputs of RG and CttM are mapped to give an understanding of generic cybersecurity threats and those unique to particular role groups. This then informs the required cybersecurity knowledge relevant to those roles (rRK).

After establishing the user's existing cybersecurity knowledge (vPK) and their role-relevant knowledge (rRK), a kind of gap analysis is performed (mapping of vPK and rRK) to then identify knowledge gap and recommend required training (RT). It is important to note that each of the components in Fig. 3 could form a branch of research on its own. Fig. 4 shows the general process of generating training recommendations.

The subprocesses referenced in Fig. 4 have been explained above but full details are omitted here. CAP uses a relational database which makes it flexible to be managed,

allowing entities such as questions, topics, or roles to be amended quickly, through an admin panel, based on feedback, without a full rebuild and deployment of the system.

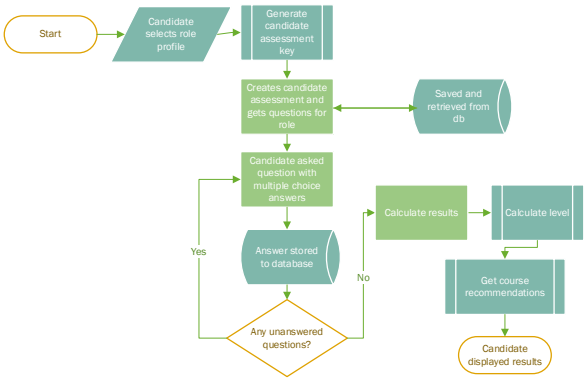

Fig. 4. User assessment flow diagram.

The design presented her is used to implement a web-based prototype in Section 4.

4 CAP Implementation and Analysis

CAP is implemented as a role-based assessment system that allows users to take a cybersecurity skills assessment based on their role. Following an assessment, users are recommended tailored training course(s) based on their level and performance. The prototype, presented here, provides the basis of a system that could be further developed into a product. It is web based and uses a database backend, along with an admin panel to allow configuration of user assessments, roles, courses, questions, topics, and levels.

For the prototype, and to manage the scope of the study, only two roles (*Data Analyst* and *Web Developer*) and three knowledge levels are used for proof of concept. The subset of topics and levels used are based on CIISec's framework sections [23]. The CAP levels are; Level 1 – Basic knowledge of principles, Level 2 – Working knowledge and understanding, and Level 3 – Expert. Questions around topics are written to be scenario and competency based, giving users four possible answers with one-best-answer. Four possible answers and a single correct response makes the probability of a user correctly guessing an answer 25% and incorrectly choosing a distractor 75% [31].

4.1 CAP – User Viewpoint and Admin Configuration

Fig. 5 shows the prototype system's homepage. Job roles are displayed from the database job roles table, with an image relating to the role to make the system more visually appealing. This is where users first choose the role closest to their job to begin the assessment process. Once a role is selected, a pre-assessment screen that confirms the chosen role name along with a unique user assessment code is displayed. Users can

use this code in future to continue an assessment or access their results, if they have already completed it, using the *Existing Assessment* menu page. Once the user starts the assessment, they are asked a series of multiple-choice questions. Only one question is asked at a time to not overwhelm the user and lower the user experience which could result in them performing less than they normally would [32].

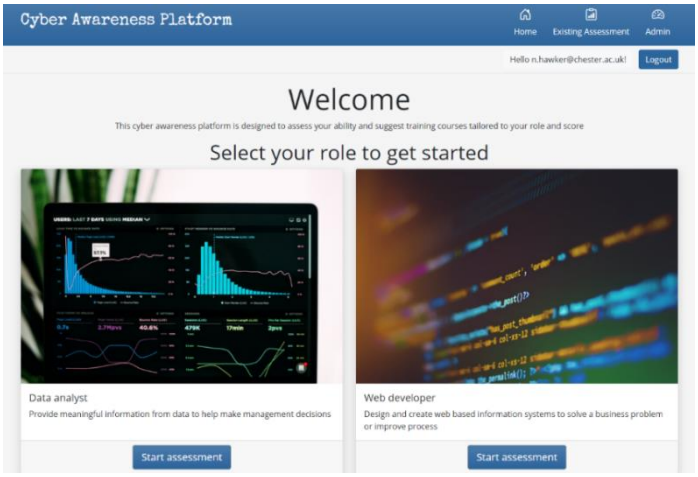

Fig. 5. CAP prototype role selection homepage.

Once the user has finished answering all the questions required for their role, they are taken to the results page which is made up of several sections starting with their determined level followed by recommended cyber training courses based on their performance. Statistics are shown providing how long they took and how many questions they answered correct/incorrect as well as the total. A *Results* section lists the possible levels followed by their overall percentage and the determined level. A *Topic analysis* section shows a radar chart listing all the topic areas assessed and the user's performance for each out of 100%. This helps visualise the user's result which can be important for visual learners as one of the four perceptual preferences for input of information [33]. A *Scoring criteria and topic level analysis* card explains the scoring formula, followed by the percentage correct by topic at each level and level total. This provides a clear way to see which areas they performed well in and those that have room for improvement. If the user did not score 100% then an *Incorrectly answered questions* section is shown. The answer the user selected is marked as well as the correct response shown in green text. This allows the user to see where they went wrong and learn the correct answer.

The system can be configured using an administrator account through a secure area. Administrators can see attempted and/or completed assessments. There are also functions to delete and access the results or manually continue the assessment if it is not complete. When creating or editing a role, the topics that apply to that role can be assigned. This is how a candidate's assessment knows which questions to use as these are attached to topics and then to roles through the relational database design. One of the

important parts of CAP is the ability for administrators to manage the question bank for assessments. The flexibility of being able to amend questions and answers easily is important for CAP to be adaptable and user friendly.

Relevant security considerations are also made. For example, ASP.net Core's Identity package, currently considered one of the secure password hashing algorithms that makes it harder to brute force passwords [34], was used to implement the login functionality to secure the administrator area. The system also protects against cross-site request forgery (CSRF) by using ASP.net core's automatic forms protection for POST requests. This means a hard to guess verification token is generated by the server-side code that is tied to the user's session and placed in a hidden field as shown in Fig. 6. When the user submits the form, the code is validated to check if it is valid for that user, if it is not correct the form data is not processed, and an exception occurs. This protects both the application and the user from a malicious actor trying to post form data from third party web page [35].

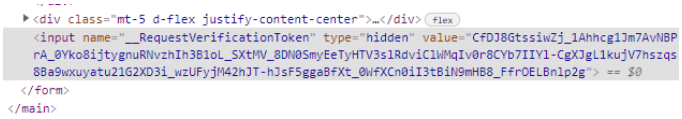

Fig. 6. CAP CSRF protection showing the unique request token in the HTML source.

4.2 Testing, Results, and Analysis

As part of this study, a cyber awareness survey was conducted to gauge the current state of cyber awareness within organisations. This helped with making informed decisions about the design of CAP. 106 participants, from 30 different sectors (majority of 38% from higher education) responded to the survey. On the need for tailored versus generic cyber training, a strong 94% agreed that '*tailored cyber training that respects my current knowledge, skill set and role would be beneficial to me*'. Considering the sample size and spread of participants in this survey, this makes a reasonable case for CAP.

Three participants took part in testing the CAP prototype, of which two were Web Developers and one was a Data Analyst. All were employed in the higher education sector. Two participants had prior cyber training and all considered themselves cyber aware. Two participants felt that CAP provided an accurate representation of their knowledge and possible training solutions for their knowledge gaps. One participant felt it was unclear how the levels were determined and made suggestions that the system could explain the calculation and criteria for levels. Table 2 shows the post-assessment question findings which were mainly positive. Notably, all three participants agreed they can see the benefit of using such a system in the workplace. One of the web developers scored 91.7% in the assessment but was capped at level one because their data security score was 50%. As a result, they were recommended GDPR and Data Protection training. Additionally, a PCI DSS Awareness course was recommended for being at level two within the secure systems development topic area.

This is a limited result as we cannot draw conclusions from a test of just three participants. However, this is a meaningful proof of concept on which to build.

Table 2. CAP prototype participant post assessment question findings. Three participants in all.

Post assessment statement	Findings
I felt confident using the system	All agreed or strongly agreed
The system was user friendly and intuitive to use	All agreed or strongly agreed
The design (look and feel) of the system was appealing	2 agreed whilst 1 disagreed
I felt that the system was accessible	All agreed
I can see the benefit in CAP being used in the workplace	All agreed
Training courses suggested are of interest and relevance to my role	2 agreed whilst 1 disagreed

Following the feedback from participants, several improvements were made to the system. These include:

- design, colour, and styling improvements; displaying the scoring criteria with the topic/level breakdowns to help candidates understand their result further;
- adding incorrect questions to the results page highlighting the candidate's response and the correct answer;
- and promoting recommended training courses to the top of the results page, so it is clear what the candidate needs to 'do', followed by their assessment outcome showing 'how' they got those recommendations, and lastly the 'why' showing their incorrect responses.

Opportunities have been, and will continue to be, identified for future CAP improvements. This will include explanations for each wrong and correct answer to help educate the candidate on the reasoning. Also, future work will include surveying a larger and more represented potential user group and detailed usability test with significant number of participants. With such improvement, more accurate conclusions can be drawn.

5 Conclusion

This study was undertaken to contribute towards improving cyber awareness and training within organisations and therefore reduce successful cyber incidents. The aims include developing a system that can assess a person's cyber awareness knowledge and identify gaps whilst considering their role profile and pre-existing skills to help companies organise efficient and fit for purpose training recommendations replacing the '*one-size-fits-all*' approach as advocated by [9, 20]. The CAP prototype does this by allowing Web Developer and Data Analyst employees to be assessed and provided with links to suitable courses dependent on their assessment outcomes. In CAP, questions are tied to topics, levels, and roles which allows candidates to be assessed at a topic level and make training recommendations based on these. Whilst this study concentrated on two role-profiles, generic recommendations can be made that apply to all roles and should be considered in cyber awareness and training.

A key limitation of the work is the few roles available for assessment as well as the depth the role profiles go into. However, this study has put in place the fundamental mechanisms for future work to be carried out to build-up more role profiles as well as

higher assessment levels. It is hoped that this study would further research in this area. With additional improvements to the CAP prototype system, and detailed test with more participants, we intend to develop an all-in-one product from assessment to training employees based on identified needs in future. As the COVID-19 pandemic has increased demand for remote working, it is vital that effective cyber training is delivered to protect organisations.

References

1. VMware Carbon Black. (2020). Global Threat Report. Retrieved 05/04/22, from https://bit.ly/3LJ9gnk
2. Rankin, B. (2018). Examining the Total Cost of Ownership of a Network Intrusion Detection System. Retrieved 05/04/22, from https://bit.ly/3uae4MD
3. IBM. (2020). How much would a data breach cost your business? Retrieved 05/04/22, from https://www.ibm.com/security/data-breach
4. Eckersley, S. (2018). The University of Greenwich - Montetary Penalty Notice. Retrieved 05/04/22, from https://bit.ly/3uOR6cY
5. Department of Health & Social Care. (2018). Securing cyber resilience in health and care: Progress update October 2018. Retrieved 05/04/22, from https://bit.ly/3LG8aZE
6. Klijnsma, Y. (2018, 11th September 2018). Inside the Magecart Breach of British Airways: How 22 Lines of Code Claimed 380,000 Victims. RiskIQ. https://bit.ly/3j9JI6S
7. He, W., & Zhang, Z. (2019). Enterprise cybersecurity training and awareness programs: Recommendations for success. Journal of Organizational Computing and Electronic Commerce, 29(4), 249-257. doi:10.1080/10919392.2019.1611528
8. Regner, S., Jordi, S.-R., Victor, C., & Jeimy, J. C. M. (2019). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Journal of Cases on Information Technology (JCIT), 21(3), 26-39. doi:10.4018/JCIT.2019070102
9. Hancock, J. (2020). Psychology of Human Error: Understand the mistakes that compromise your company's cybersecurity. Tessian Research. https://bit.ly/3Lzn1Fg
10. Jolly, J. (2020). Huge rise in hacking attacks on home workers during lockdown. Retrieved 05/04/22, from https://bit.ly/3NMq4vJ
11. NCSC. (2019). 10 steps to cyber security - Common cyber attacks - reducing the impact. Retrieved 05/04/22, from https://bit.ly/3LJK3cs
12. Chapple, M., Stewart, J., & Gibson, D. (2021). Certified Information Systems Security Professional Official Study Guide. Pp 96-98. 9th Edition. John Wiley & Sons, New Jersey
13. HM Government. (2016). National Cyber Security Strategy 2016-2021. https://bit.ly/3J5mI3r
14. Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H. N. (2020). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems, 1-16. https://doi.org/10.1080/08874417.2020.1712269
15. NCSC. (2021, 14 April 2021). NCSC's new cyber security training for staff now available. National Cyber Security Centre. https://bit.ly/3DHRlL6
16. Axelos. (2015). RESILIA® Cyber Resilience Best Practice. TSO (The Stationery Office)
17. McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. Computers in Human Behavior, 69, 151-156. https://doi.org/10.1016/j.chb.2016.11.065

18. Pattinson, M., Butavicius, M., Lillie, M., Ciccarello, B., Parsons, K., Calic, D., & McCormac, A. (2019). Matching training to individual learning styles improves information security awareness. Information & Computer Security, 28(1), 1-14. https://doi.org/10.1108/ics-01-2019-0022
19. Shinoda, Y., Tan, Y., Chinen, K.-i., Tang, D., Pham, C., & Beuran, R. (2017). CyTrONE: An Integrated Cybersecurity Training Framework Proceedings of the 3rd International Conference on Information Systems Security and Privacy
20. Elvey, C. A. (2020). Policing the UK Cyber Threat: Developing Education and Training for the Front Line. University of Chester.
21. Oyinloye, T. A. (2019). Towards Cyber-User Awareness: Design and Evaluation. University of Chester.
22. MITRE. (2017). Cybersecurity: Awareness & Training. The MITRE Corporation. Retrieved 05/04/22, from https://bit.ly/38joAbU
23. CIISec. (2018). CIISec Skills Framework. https://www.ciisec.org/Skills_Framework
24. SFIA. (n.d.-a). Digital Transformation Skills in SFIA. Retrieved 05/04/22, from https://sfia-online.org/en/assets/documents/sfia-view-of-digital-transformation-skills.pdf
25. Watkins, R., West, M. M., & Visser, Y. (2012). Guide to assessing needs: Essential tools for collecting information, making decisions, and achieving development results. World Bank Publications. https://ebookcentral.proquest.com/lib/uocuk/detail.action?docID=868308#
26. SFIA. (n.d.-b). Everyone has information security responsibilities. Retrieved 05/04/22, from https://bit.ly/3r5sxrc
27. SFIA. (n.d.-c). Mapping SFIA skills to NICE work roles. Retrieved 05/04/22, from https://bit.ly/3j510Sr
28. NICCS. (2021, 29th July 2021). Workforce Framework for Cybersecurity (NICE Framework). Retrieved 05/04/22, from https://bit.ly/35Gda10
29. Rashid, A., Chivers, H., Lupu, E., Martin, A., & Schneider, S. (2021). The Cyber Security Body of Knowledge, Version 1.1.0. https://www.cybok.org/media/downloads/CyBOK_v1.1.0.pdf
30. Kirwan, B., & Ainsworth, L. K. (1992). A guide to task analysis: the task analysis working group. CRC press.
31. Hingorjo, M. R., & Jaleel, F. (2012). Analysis of one-best MCQs: the difficulty index, discrimination index and distractor efficiency. J Pak Med Assoc, 62(2), 142-147. https://www.ncbi.nlm.nih.gov/pubmed/22755376
32. Garrett, J. J. (2010). Elements of User Experience,The User-Centered Design for the Web and Beyond. Pearson Education.
33. Leite, W. L., Svinicki, M., & Shi, Y. (2009). Attempted Validation of the Scores of the VARK: Learning Styles Inventory With Multitrait–Multimethod Confirmatory Factor Analysis Models. Educational and Psychological Measurement, 70(2), 323-339. https://doi.org/10.1177/0013164409344507
34. 1Password. (2021, 12th August 2021). https://support.1password.com/pbkdf2/
35. Hasan, F., Anderson, R., & Smith, S. (2022). Prevent Cross-Site Request Forgery (XSRF/CSRF) attacks in ASP.NET Core. Microsoft. Retrieved 05/04/22, from https://bit.ly/3x6oLSc