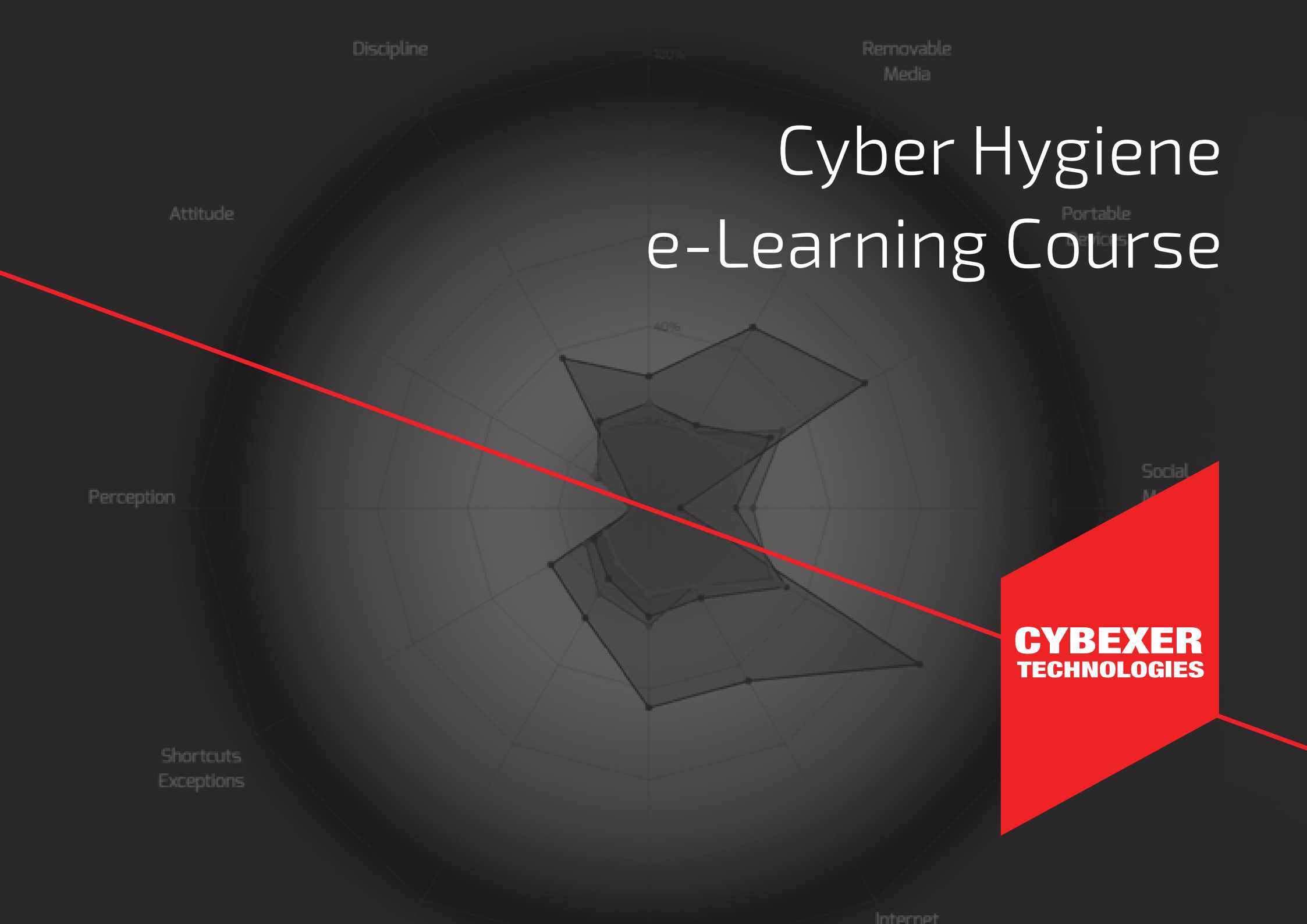


Cyber Hygiene e-Learning Course

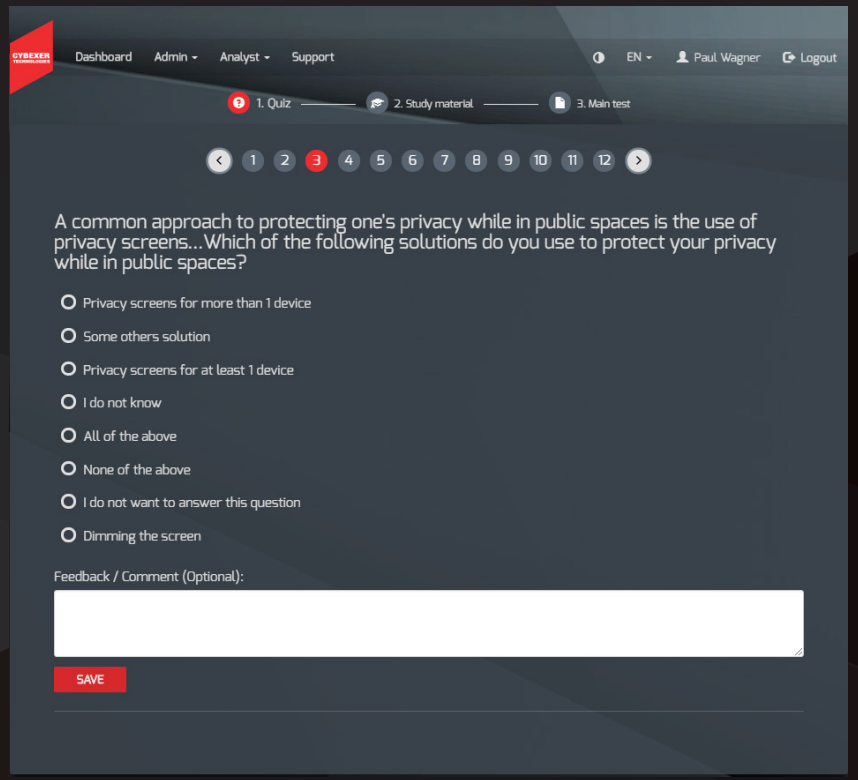
CYBEXER TECHNOLOGIES

Cyber Hygiene e-Learning Course

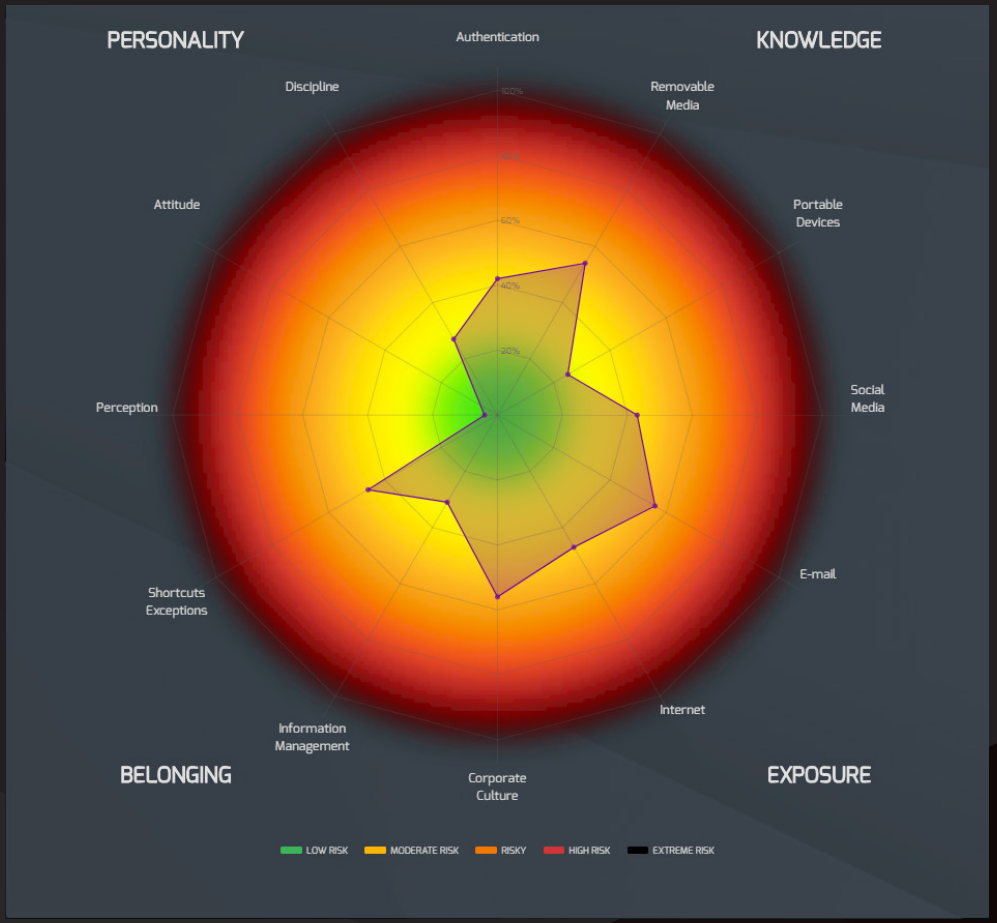
- The Cyber Hygiene e-Learning Course is an interactive, engaging and effective tool consisting of a training module and two separate test modules to address human risk behaviour in cyberspace.
- The Cyber Hygiene e-Learning Course targets three categories of staff members (managers, regular users and specialists) and addresses specific concerns and threats associated with each of these groups.
- The course can also serve as an effective risk-mapping tool because it collects feedback from the participants as they react to the issues they face. Based on these reactions, the tool is highlighting the risk areas of each participant. The results can be further aggregated to teams and whole organisations. The goal of this multi-level analysis is to facilitate the implementation of security policies, decision-making processes and effective risk mitigation.

Concept

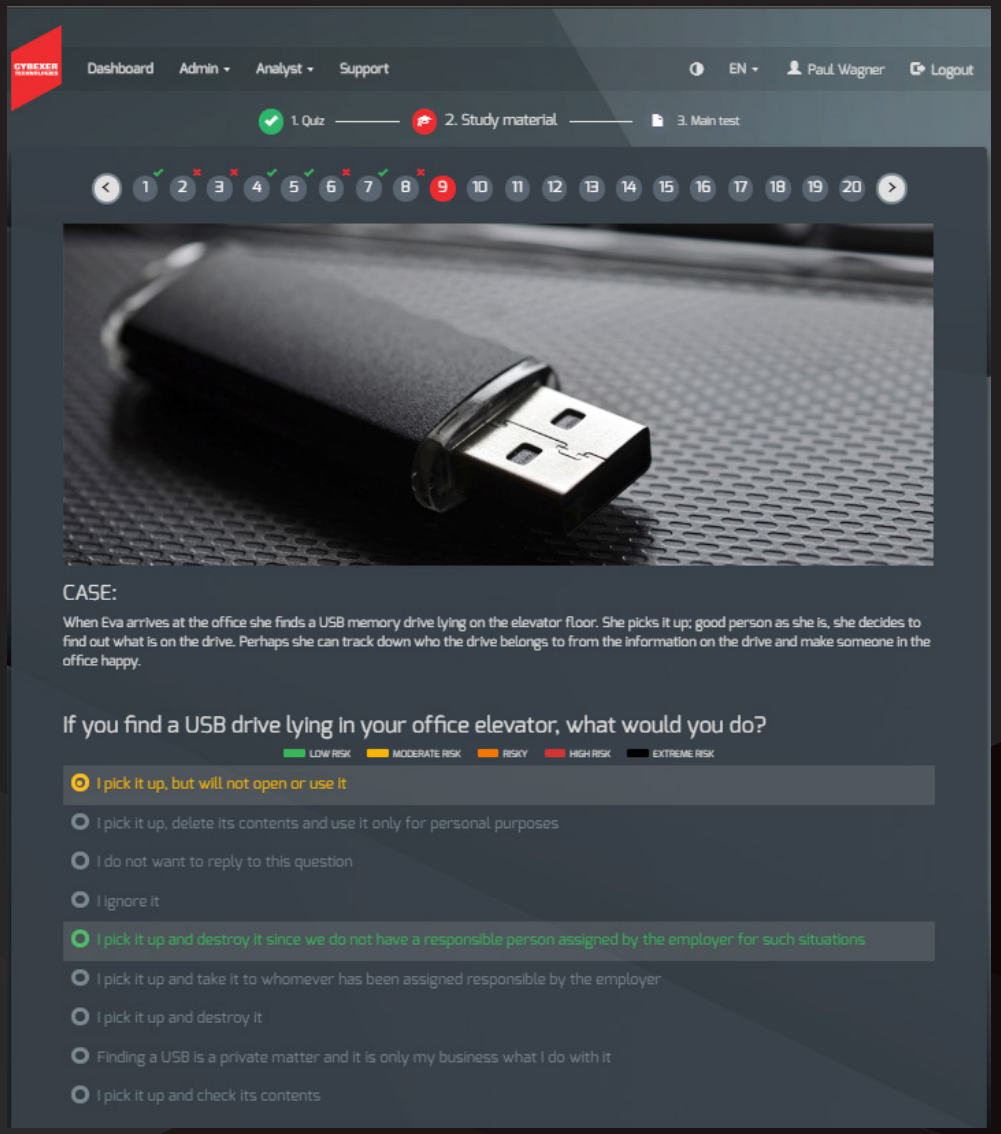
- Our concept is based on the notion that human risk behaviour management in cyberspace is a continuous process in which trainees and instructors alike need to learn and adapt. The course is based on a project first implemented by the Estonian and Latvian ministries of defence and the European Defence Agency as a direct response to sophisticated, targeted cyber-attacks. This particular defence programme was developed and implemented over 2015-2017. Following its success in the defence sector, the course was adjusted for wider commercial use, including export.
- During the development of the course, several other cyber awareness courses were analysed and our approach is based on principles that aim at preventing the shortcomings that hamper achieving effective results. The principles are briefly described below.



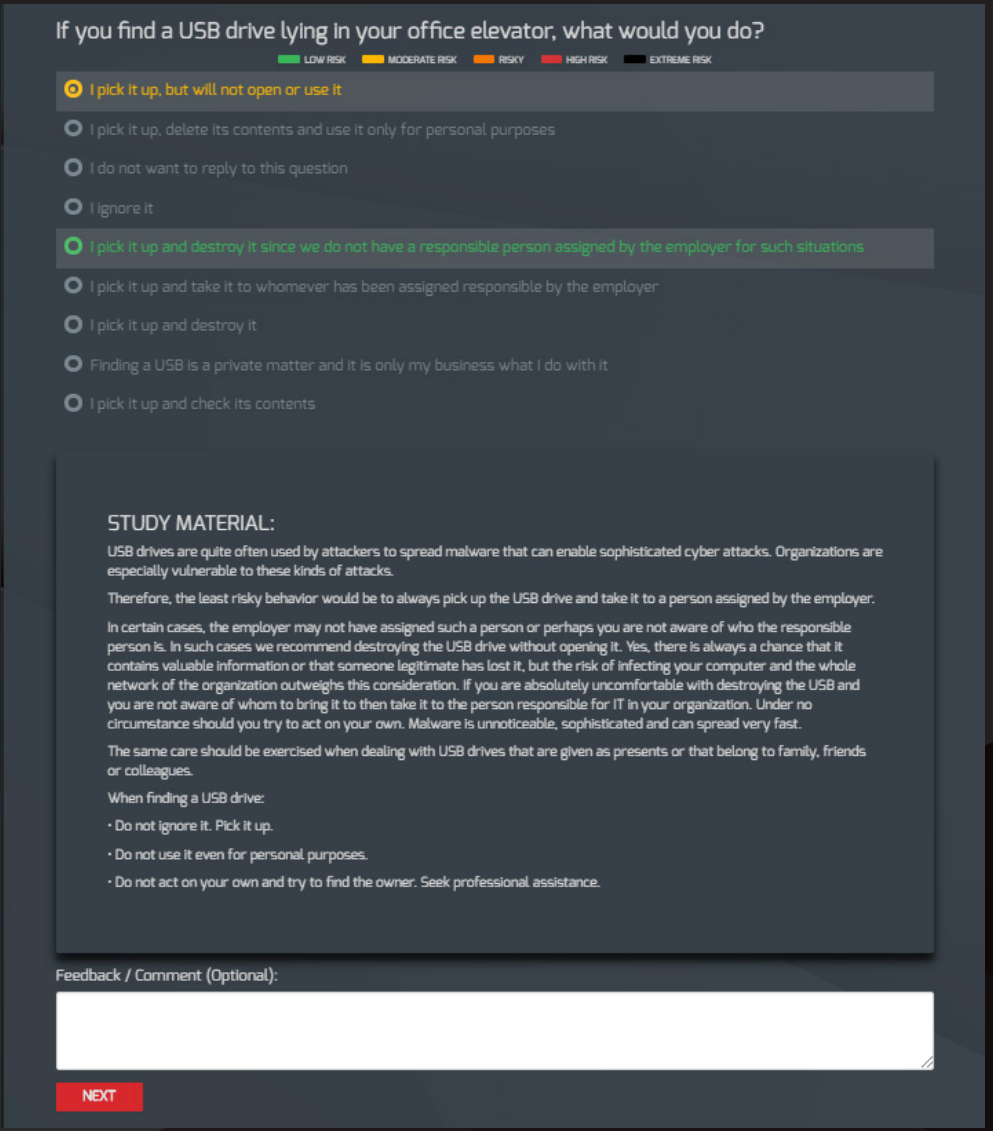
- **No “pass or fail”.** The course is not “pass or fail”. Instead, it seeks to identify specific risk areas in which the participant may be affected. For example, a person participating in a typical “pass or fail” scored course may attain a score of 90%, but this does not address the 10% which are a part of the risk behaviour profile of that person. This, in turn, may lead to a false sense of security while the person might not even be aware of this critical vulnerability.
- **Systemic Risk Matrix.** The participants are assessed against a systemic risk matrix in which the level of risk along each threat vector is highlighted. The risk matrix does not only refer to technical aspects but also describes issues related to the individual and the organisation as a whole. A detailed discussion of the approach of the risk matrix is discussed below.
- **Interaction.** The course is interactive: the participants need to react to the situations and questions with which they are presented during the course. In addition to understanding the individual risks of the participants and the threat profile of the entire organisation, this approach is an effective way of keeping the course dynamic and responsive.



- **Feedback.** In addition to general interaction, we ask participants to provide feedback as well. In every given scenario, the participants can share their stories and experiences anonymously and may note disagreements or comments that they deem necessary. All of this helps us to stay in touch with the real world. Our experience so far has shown that this feature is extremely useful: often the instructors fail to imagine some of the areas that need addressing, differences in attitude to security or imaginative "shortcuts" that people have devised in dealing with security.
- **"The Firewall Approach".** The course is constantly updated and new releases are issued regularly on the basis of the respective global, country or industry-specific threat background. The regularity of the course and updates help to create a "human firewall" within organisations which form the ultimate line of defence against cyber-attacks.



- **Creating a Community.** With our methodology, we are also striving to create a community of responsible organisations. A user portal for CISOs and cyber hygiene project managers will be launched shortly. It will become an environment for discussing the features and content of the course, receiving user feedback, requesting and suggesting updates, sharing obfuscated data and trends, and other options. The community supports our understanding of cyber hygiene as a constantly evolving process in which new threats need to be addressed quickly. We also organise annual user conferences to address new trends, ideas and features in greater detail. We want to make sure that our clients are heard: such feedback can be invaluable for establishing safer computer practices in all organisations.

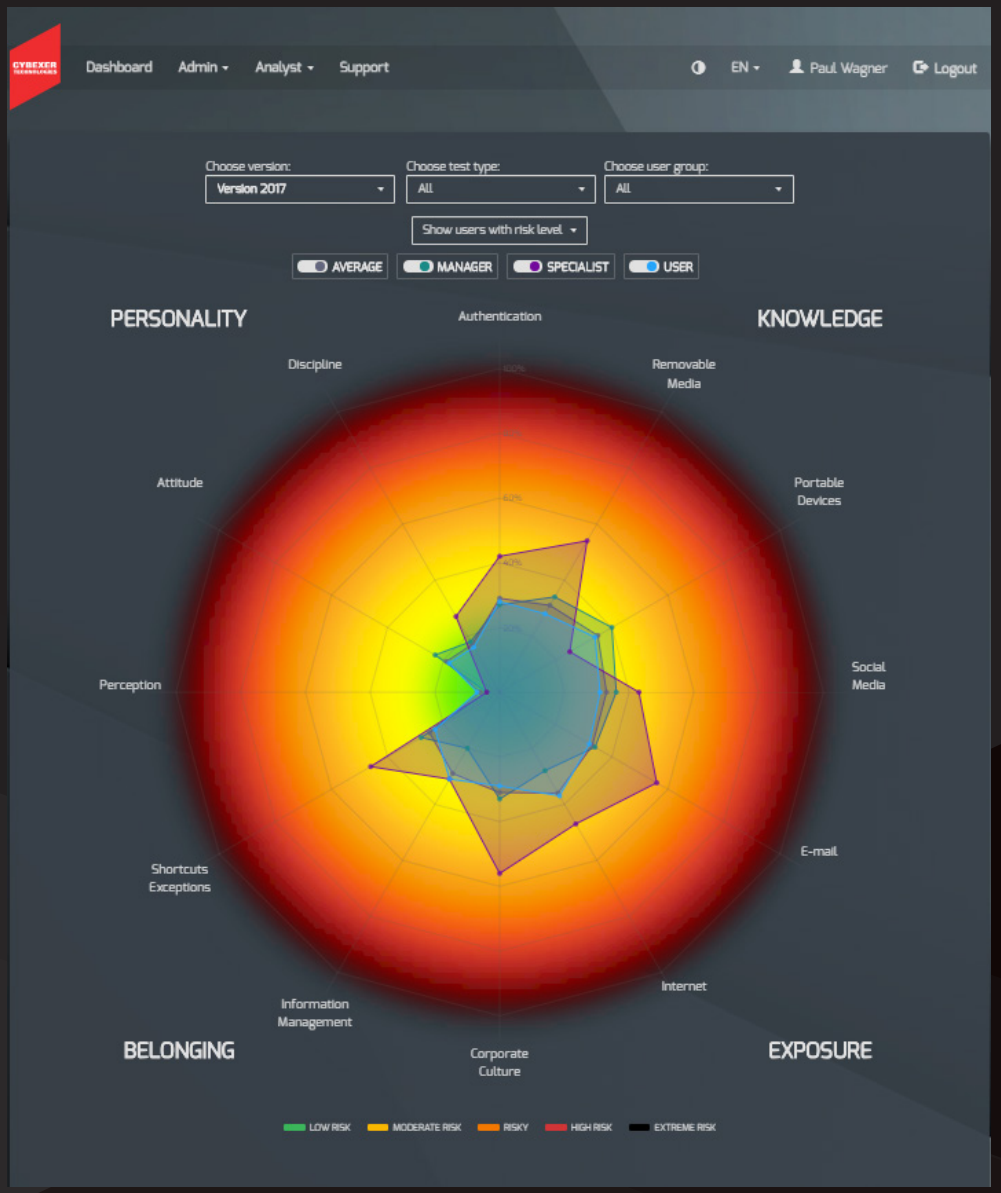


Risk Matrix

The individual cyber hygiene profile is generated on the basis of the answers which the participants provide throughout the course. The profile is based on the risk matrix which is also a foundation for the development of the course material and tests. It is important to remember that our understanding of and approach to human risk behaviour is still evolving and that there is a lot to improve. Bearing this in mind, we have decided to use the following matrix as our starting point.

We have divided the human risk matrix in cyberspace into four parts: (1) “Personality”; (2) “Knowledge”; (3) Exposure”; (4) “Belonging”.

- The **“Personality”** part of the risk profile helps to tell us who we are as individuals and, obviously, this is the most complex part of the profile. “Discipline” shows how actively a user is willing to act in the name of safety precautions. “Attitude” shows the person’s overall understanding of the risks surrounding computers, smart devices and the internet. “Perception” refers to the person’s openness to helping enact security measures in real life situations by implementing the topics covered in the course.
- The **“Knowledge”** part of the profile shows how well the participant understands technology and security. This part includes authentication, removable media, portable devices, etc.



- The **“Exposure”** part of the profile shows the risks that the participant is exposed to in cyberspace such as social media, e-mail and web pages.
- The **“Belonging”** part of the profile demonstrates the degree of risk to which the participant is exposed within the organisation. This part deals with the corporate culture, information management and tolerance of security shortcuts/exceptions within the organisation.

Ability to understand risk

- It is important to understand that our solution is not simply a passive awareness course but an effective tool at the CISO's disposal. First of all, the tools give an understanding of human risk behaviour within the organisation as well as in particular teams, departments and/or different branches. The results help the management make decisions regarding investments, additional training or potential changes in security policies. Due to our community approach, CISOs can always stay up to date with recent risks, discuss with peers and assess the cyber security awareness level of the organisation.
- Within our user community, we have established a working group of CISOs to further develop and refine the “CISO dashboard” on cyber hygiene. This working group constantly adds improvements and new features to the dashboard.
- The system supports regular reporting to management on an annual, quarterly or monthly basis. This is a valuable method of interaction with the management structures of the organisation and presents a comprehensive risk overview.
- The system supports overall risk management progress and can be particularly helpful with liability insurers in assessing risks because human behaviour-related cyber risk is typically extremely hard to quantify.

Staying up to date

- The course is regularly updated on the basis of the latest trends in cyber security, customer feedback and requirements.
- We cooperate with several government agencies and private sector institutions to keep ourselves informed about the ever-changing threat landscape in cyber security.
- Content updates are released regularly: first, immediately after a major event or incident requiring additional training has occurred or is about to occur; second, at least once a year in a bundle developed on the basis of the analysis by our team of experts.
- We are also updating the course regularly in order to stay user-friendly and practical. Currently, we are developing a number of new features (e.g. a statistical module, visual aids, a comment section, etc.) that will make the e-learning experience engaging and worthwhile.

Benefits of the course for your organisation

- Effective information protection by promoting responsible human behaviour and avoiding exposure to threats from cyberspace.
- Understanding the weaknesses and vulnerabilities of your organisation by analysing the course results.
- Staying compliant with international information security standards.
- Informed decisions by the management based on the feedback and analysis of the course results.
- Being prepared for the latest threats as the course is regularly updated to take into account the developments in the realm of cyber threats.

Product deployment

The Cyber Hygiene e-Learning Course is easily deployable. It can be implemented in any organisation within days, taking into account all security and IT infrastructure requirements.
The course runs on the CybExer Technologies OÜ's proprietary platform. CybExer Technologies will not have any access to user data or user profiles. This information remains with the Client. If the Client wishes to share such information in any way (for user conferences, feedback, scientific research), it will be only accepted in an obfuscated form to ensure compliance with European data protection regulations.

Deployment steps:

- Online workshop to identify infrastructure requirements.
- On-site workshop on the required customisation, introduction and use within the organisation, installation and implementation. This workshop is meant for up to 10 people including a focus group to validate the contents of the course.
- The administrator should be able to administer the course, using the provided user guide and support from the CybExer Technologies Support team.

Cyber Hygiene e-Learning Course workshop

The workshop will take place at the Client's premises and will usually last 1-2 working days.

Implementing the Cyber Hygiene e-Learning Course

- Introduction, general overview of the Cyber Hygiene project and Cyber Hygiene Standard Document.
- Validation of the contents of the course
  - It is crucial to validate that the contents of the course meet the policies and requirements of the organisation. It is equally important that the course would take into account various cultural and other client-specific circumstances. Although it is intended to be an off-the-shelf solution, certain customisation and regard to client requirements are possible during the implementation phase.
  - The ideal way to validate the course would be to run it with an internal focus group selected by the organisation. The required time should not exceed 2 hours for both the course and feedback session. The feedback will then be further discussed and potential changes shall be agreed upon with the Client's project manager/project team.
- Introduction of the course within the organisation
  - This part consists of a discussion and brainstorming session on how to better introduce the course within the organisation.
  - During this stage, the experience of introducing the course in other similar organisations can be discussed more widely.
  - Mitigating human risk behaviour in organisations is an important task, and this segment of the workshop will address the ways how to best achieve this task.
  - The course will also offer valuable statistical and other information: the users will be briefed on how to make the best use of the data that will be available to them upon completing the course.

Technical introduction of the e-learning platform

- How to troubleshoot in case of technical problems.
- Introduction of documentation and specifications.
- Implementation of the course within the organisation.
- Update, customisation and renewal processes.