UNIVERSITY OF TARTU
Institute of Computer Science
Computer Science Curriculum

Marco Kuusk

Cyber Hygiene Feedback Tool

Bachelor's Thesis (9 ECTS)

Supervisor:
Arnis Paršovs, PhD

Tartu 2025

Cyber Hygiene Feedback Tool

Abstract:

This bachelor's thesis presents the design, implementation, and evaluation of an automated cyber hygiene feedback tool aimed at helping organizations of all sizes improve their cybersecurity posture. The objective was to create a lightweight, web-based self-assessment tool that enables both employees and organizational representatives to identify security gaps and receive actionable recommendations without requiring technical expertise.

The tool consists of two structured questionnaires, one for individuals and one for organizations, and a user-friendly web interface. Responses are analyzed using a scoring model and processed by a feedback engine that combines rule-based logic with generative AI (OpenAI GPT-4o). The result is a detailed report outlining strengths, weaknesses, risk scenarios, and a time-bound action plan.

The feedback tool was evaluated through simulated data and real-world use. One organization used the system twice, first for assessment, and later for re-evaluation after implementing recommended improvements, and increased its cyber hygiene score by 13 percentage points. In total, six employees used the tool; three of them re-evaluated themselves after making concrete changes. All of these re-evaluations resulted in an average increase of 9.6 percentage points in their scores. These results suggest the system is effective in increasing awareness and supporting measurable security improvements.

Keywords: cyber hygiene, cybersecurity awareness, AI-generated feedback, self-assessment, risk reduction, feedback system

CERCS: P170 Computer science, numerical analysis, systems, control

Küberhügieeni tagasiside tööriist

Lühikokkuvõte:

Käesolev bakalaureusetöö kirjeldab küberhügieeni tagasisidesüsteemi loomist, rakendamist ja hindamist, mille eesmärk on aidata igas suuruses organisatsioonidel parandada oma küberturvalisust. Eesmärk oli arendada kerge ja kasutajasõbralik veebipõhine enesehindamise tööriist, mis võimaldab nii töötajatel kui ka organisatsioonidel tuvastada turbeprobleeme ning saada praktilist ja arusaadavat tagasisidet ilma tehnilise taustata.

Süsteem koosneb kahest struktureeritud küsimustikust, üks individuaalsele kasutajale ja teine organisatsiooni tasemele, ning lihtsast veebiliidesest. Vastuste alusel arvutatakse skoor ja käivitatakse tagasiside generaator, mis kasutab reeglipõhist loogikat ja generatiivset tehisintellekti (OpenAI GPT-4o). Lõppresultaadiks on raport, mis sisaldab tugevusi, nõrkusi, riskistsenaariume ning ajaliselt jaotatud tegevuskava.

Tööriista hinnati nii simuleeritud andmete kui ka praktilise kasutuse kaudu. Üks organisatsioon kasutas süsteemi kahel korral, esimesel korral hindamiseks ja teisel korral korduvhindamiseks pärast soovituste rakendamist, ning parandas oma tulemust 13 protsendipunkti võrra. Kokku kasutas tööriista kuus töötajat, kellest kolm tegid pärast parenduste elluviimist kordushindamise. Kõik kordushindajad saavutasid keskmiselt 9.6 protsendipunkti suuruse tõusu oma tulemustes. Need tulemused näitavad, et süsteem on tõhus ja aitab kaasa teadlikkuse tõusule ning mõõdetavale turvalisuse parandamisele.

Võtmesõnad: küberhügieen, küberturvalisuse teadlikkus, tehisintellekti tagasiside, enesehindamine, riski vähendamine, tagasisidesüsteem

CERCS: P170 Arvutiteadus, arvutusmeetodid, süsteemid, juhtimine

Contents

1. Introduction

With growing size and complexity of cyber attacks, organizations of all sizes are forced to embrace good cyber hygiene practices to protect their systems, data, and personnel [1, 2]. However, many organizations, particularly those without dedicated information technology personnel, find it difficult to evaluate and enhance their cybersecurity stance due to technical complexity and limited availability of existing tools and criteria [3, 4].

This thesis documents the development of a lightweight, web-based cyber hygiene self-assessment and feedback tool made to help organizations and employees evaluate their cybersecurity readiness without requiring technical expertise. As result of this work, two structured self-assessments were created: one focusing on organization-level practices and the other on individual employee behaviors. Upon completion, organizations may download an automatically generated, personalized portable document format (PDF) report that includes a cyber hygiene score, key strengths, areas for improvement, potential risks, and a prioritized action plan.

The tool developed in this thesis addresses a gap identified in the existing landscape of cybersecurity resources. It uses a simple yet effective architecture to support both technical and non-technical users. The interface is intentionally minimalistic and intuitive, requiring no prior training, while the feedback is structured to be clear, practical, and actionable. This makes the tool accessible to a wide range of organizations regardless of their size or internal cybersecurity expertise.

Unlike existing frameworks, which often rely on static checklists or require expert knowledge [5], this tool emphasizes usability, simplicity, and applicability. It translates self-reported answers into meaningful insights using a combination of rule-based logic and natural language generation powered by OpenAI's GPT-4o model [6]. This hybrid design enables automated feedback that is both personalized and easy to understand — qualities largely absent in comparable tools [7, 8].

The tool developed in this thesis is intended to support both technical and non-technical users across organizations of varying cybersecurity maturity levels [3]. It is designed to be accessible to small businesses without dedicated IT staff, while also offering meaningful guidance to more technically capable organizations. By generating structured, actionable feedback based on self-assessment data, the tool aims to help users identify key strengths, weaknesses, and risk areas. Although it is not a replacement for professional audits or penetration testing, it will

lower the barrier to entry for organizations seeking to evaluate and improve their cyber hygiene independently and affordably [9].

OpenAI's GPT-4o model was also used during the writing of this thesis to assist in structuring sections into LaTeX format, correcting grammatical errors, identifying repetition, and rephrasing complex sentences for clarity.

2. Background and Related Work

This section talks about the context and motivation behind the thesis, reviews existing information security frameworks, cyber hygiene self-assessment tools, cybersecurity awareness platforms, and related resources. The aim is to identify their strengths and limitations, especially in terms of usability, personalization, and accessibility. This review provides the necessary context for understanding why a new tool was developed and how it differs in approach and functionality.

2.1 Context and Motivation

Although a variety of cybersecurity assessment and training tools exist, many organizations, particularly those without dedicated informaion technology (IT) staff, struggle to find resources that are both effective and accessible. Existing solutions typically fall into two categories: technical tools intended for expert use, or awareness-focused platforms aimed at education and quizzes [10]. While some tools such as ENISA's assessment platform [11] and the Cyber Readiness Institute (CRI) program [12] attempt to bridge the gap, they often fall short in terms of usability, reliability, or personalization.

Most also fail to offer tailored, easy-to-understand, and actionable feedback — often presenting results that require technical interpretation or offering overly generic guidance that does not account for the user's specific context or technical maturity level [4, 10]. This thesis was motivated by the lack of lightweight, self-guided tools that deliver actionable, context-aware security feedback without requiring technical expertise. The goal was to help organizations understand and improve their cyber hygiene independently, without relying on costly consultants, technical audits, or complex training programs.

To design a solution that addresses these limitations, it was important to understand the strengths and weaknesses of existing feedback models. Traditional cybersecurity tools often use rule-based logic, where each answer maps to a fixed outcome. These systems are fast, simple, and consistent, which makes them appealing for environments requiring reliability. However, they are also rigid and unable to adapt to nuanced or context-specific input [13, 14]. The scoring component of this tool follows a similar rule-based approach to ensure transparency and consistency, but it is complemented by AI-driven feedback generation to provide flexibility and personalization.

By contrast, artificial intelligence (AI) powered systems, especially those built on large language models, can generate personalized, natural language feedback. These systems adapt their tone, prioritize risks dynamically, and provide feedback that feels more human and relevant [7, 8].

However, AI tools can also be unpredictable or vague if not carefully prompted, and may struggle with structure or consistency without proper input formatting [15].

2.2 Information Security Frameworks

Several information security frameworks serve as foundational models for cybersecurity evaluation. The **NIST Cybersecurity Framework (CSF)** [16] and **ISO/IEC 27001** [17] provide comprehensive methodologies for managing and improving information security. These frameworks are widely respected and form the basis of many organizational policies. However, they are typically documentation-heavy and designed for organizations with the capacity to support dedicated IT or compliance teams [18]. Their implementation requires both technical competence and time, which may not be feasible for all organizations [18].

More accessible options include the Estonian **E-ITS framework** [19], which present security practices in a more digestible format. Even so, applying recommendations effectively still demands familiarity with cybersecurity concepts and terminology, which may present barriers for organizations with limited internal expertise [1].

Unlike these frameworks, the tool developed in this thesis does not require technical background, prior training, or interpretation of complex documentation. It was intentionally designed to be lightweight, interactive, and directly usable through a web interface. Instead of relying on abstract guidelines, the tool guides users through a structured assessment and immediately provides contextualized, plain-language feedback based on their specific answers.

While frameworks like NIST [16] and ISO [17] serve as comprehensive reference points, they are better suited for long-term governance and compliance [20]. This tool, in contrast, prioritizes clarity, accessibility, and immediate actionability — enabling organizations to start improving their cyber hygiene independently and without delay.

2.3 Security Awareness and Training Platforms

To develop a practical and effective cybersecurity self-assessment tool, it was essential to review existing awareness and training platforms. These platforms provide valuable insights into common approaches, strengths, and limitations in helping organizations and individuals improve their cyber hygiene. The following summary highlights key examples, demonstrating the gap this thesis aimed to fill.

KyberTest [21] is an educational platform aimed at organizations looking to implement internal cyber hygiene courses and assessments. It allows administrators to create custom tests from scratch or use a built-in question bank filled with pre-made questions on security topics. This flexibility makes it useful for tailoring training to organizational needs. However, KyberTest focuses primarily on learning and evaluation, not feedback. It does not generate tailored guidance or summarize results into actionable steps. As such, while it supports internal awareness programs, it does not serve as a self-assessment tool that helps organizations identify and address specific security weaknesses.

Similarly, the **Digiriigi Akadeemia** [22] platform includes self-study cybersecurity materials, but these are intended as educational courses rather than decision-making support tools. Their aim is to build baseline knowledge, not to produce individualized reports or risk classification.

The **Cyber Readiness Institute (CRI) Program** [12] takes a structured, course-based approach to improving cybersecurity awareness, especially among employees and small teams. It includes multiple modules with educational videos, short surveys, and end-of-module quizzes. While this format supports gradual learning and comprehension, it is more aligned with training than assessment. One of its notable strengths is multilingual support, offering content in English, Russian, Spanish, and Portuguese, which improves accessibility for diverse audiences. However, the program does not generate tailored cybersecurity feedback or a summarized report based on user responses. As a result, it may be less suitable for organizations looking for a quick snapshot of their cybersecurity posture or a prioritized action plan. Instead, its focus lies in structured education and awareness-building over time.

MyCyberHygiene.com [23], developed by CybExer Technologies [24], is a free cyber hygiene course aimed at individual users. It combines educational content with interactive modules, including a study section, quizzes, and basic testing. Users are guided through common cybersecurity scenarios with explanations for both correct and incorrect answers, which helps reinforce good practices. At the end of each session, a personalized profile is generated that summarizes risk levels across different cyber hygiene domains. While the tool is engaging and informative, its primary focus is awareness and behavior change rather than structured self-assessment or generating actionable feedback based on responses. Unlike the tool developed in this thesis, **MyCyberHygiene.com** does not provide a structured action plan or downloadable, tailored feedback report.

CybExer's E-learning Platform (University of Tartu Version) [25] is one of the most comprehensive cyber hygiene platforms reviewed during this thesis. It combines educational content with assessment and provides detailed, contextual feedback after each question. One of its distinguishing strengths is its use of rich visual content, including annotated examples of phishing emails and unsafe links, that help reinforce good practices. The interface supports both light and dark modes, and the platform is fully bilingual (Estonian and English), enhancing accessibility.

The system categorizes cyber hygiene into well-defined domains such as authentication, data storage, devices and networks, e-mail, social media, information management, self-discipline, and organizational culture. Users receive tailored visual reports based on their profile test, study material test, and exam test, each accompanied by explanations on how to interpret the visual charts. Each answer is immediately followed by a color-coded feedback system indicating the associated risk level (from low to extremely high), along with practical recommendations and explanations for each choice.

However, despite the strengths of its educational model, this tool lacks a personalized action plan. Its primary purpose is training and risk awareness rather than generating an actionable, time-bound improvement plan. Additionally, access to the full platform is limited to members of the University of Tartu or associated organizations, which restricts broader use.

CybExer's cyber range [24] also provides a sophisticated solution offering scenario-based, hands-on training for technical users in high-stakes environments. While effective, it is aimed at more mature institutions with training resources and facilitator support — making it less relevant to organizations seeking lightweight tools.

The tool developed in this thesis differs from these awareness and training platforms in both purpose and implementation. While platforms like KyberTest and CRI focus on education through courses, quizzes, and training modules, this tool is designed for practical self-assessment and immediate feedback. It does not aim to replace training but to complement it by identifying actual security weaknesses and generating a personalized action plan based on user responses. Unlike most training platforms, it uses AI to dynamically generate tailored PDF reports — offering actionable insights without requiring follow-up interpretation or prior knowledge. The goal was to create a lightweight, accessible tool that organizations can use independently to evaluate and improve their security posture without needing external facilitators or training cycles. This focus on self-directed improvement, rather than passive learning, makes the tool

uniquely suited for organizations looking for direct, measurable, and practical cybersecurity guidance.

2.4 Cyber Hygiene Self-Assessment Tools

Several tools aim to help organizations assess their security posture more directly. These typically consist of structured questionnaires and scoring logic that highlight potential weaknesses.

ENISA's Assessment Tool [11] stands out for its design and structured presentation. It provides clear visuals, category scores, and promises a tailored action plan and industry-specific benchmarking. However, in testing, the tool repeatedly failed to proceed to completion due to a malfunctioning "Next" button — despite all answers being filled. This occurred in all five attempts during testing over the period of a month, preventing any full report generation. While the tool conceptually offers detailed feedback, this experience suggests an urgent need for robust, user-friendly web interfaces that do not create usability barriers.

The UK's **Cyber Essentials Readiness Tool** [26] provides a structured, step-by-step self-assessment designed to help organizations better their cybersecurity posture. One particularly useful feature is the presence of action items next to certain questions — these explain relevant concepts in plain language and often suggest small improvements (e.g., "By setting a unique 6 character or more password or pin number, or a biometric method to unlock your devices, you can stop unauthorised people accessing your information if the device is lost, stolen or left unattended") while also suggesting immediate action [26]. This helps users who may not understand the technical terms used in the questions and reduces the intimidation factor while also prompting swift action.

The tool also includes a *"Save and continue later"* feature, which allows users to pause their assessment and return when ready. This is especially beneficial for overwhelmed users or those completing the questionnaire across multiple sessions.

However, despite these helpful additions, the final feedback feels static. It summarizes the user's responses and provides generic next steps, such as reviewing FAQs or joining a LinkedIn advice group. The recommendations lack personalization and do not account for the context or maturity level of the user's answers.

Additionally, the tool omits several countries, including Estonia, from its country selection dropdown, which may limit its perceived accessibility for international users. This is a

notable oversight given the tool's aim to support a broad range of organizations in improving cybersecurity readiness.

In Estonia, the **MASS** [27] tool is one of the most thorough evaluations of organizational cybersecurity maturity. However, many of its questions reflect technical expectations. Examples include:

- "Before a server is deployed, a server usage plan is drawn up..."
- "Web applications have limited access to files in a specified directory tree..."
- "Database systems are reviewed regularly. Reviews include..."
- "When reusing devices affected by a security incident..."
- "When documenting a security incident, all actions taken..."

Such questions require respondents to have intimate knowledge of internal systems and security operations — making it unsuitable for general users or organizations without dedicated IT staff.

While MASS provides graphs and visuals for interpreting results the tool lacks tailored, narrative feedback. Users must interpret the results themselves, which may result in misunderstandings or underutilization of the insights provided.

The tool developed in this thesis was designed to address the key limitations observed in these existing solutions. Unlike tools that provide static or generic feedback, this system generates dynamic, personalized reports based on the user's responses. It combines predefined scoring logic with natural language generation to create feedback that is both context-aware and easy to understand.

Whereas some tools fail to function reliably or present overly technical questions, this tool prioritizes usability by using a minimalistic web interface, simple language, and immediate feedback. Additionally, the inclusion of downloadable, AI-generated PDF reports allows organizations to retain a structured action plan without requiring expert interpretation. This approach was chosen specifically to support users without a technical background, and to make security self-assessment more actionable, accessible, and scalable.

While the tool developed in this thesis addresses many limitations found in existing platforms, particularly in terms of accessibility and personalization, it also comes with certain constraints. Most notably, the quality of the AI-generated feedback depends on the clarity and completeness

of the input data. Since users self-report their answers, the accuracy of the final report can be affected by misunderstandings, misjudgments, or lack of honesty. In addition, while the tool generates structured action plans, it does not currently track whether users implement them or measure long-term improvements. These limitations highlight the importance of treating the tool as a supportive aid rather than a substitute for professional cybersecurity guidance when deeper or more technical analysis is required.

3. Methodology

This section explains how the Cyber Hygiene Feedback Tool was developed and tested. Its purpose was to provide a simple and available instrument assisting organizations, particularly those with few IT skills, comprehend and enhance their cybersecurity stance. The procedure entailed designing two questionnaires, designing a user-friendly web interface with static feedback, and adding automated AI-driven feedback.

3.1 Approach and Rationale

A design science research approach was used [28], focusing on building and evaluating a working software solution. The problem of cybersecurity assessments being too technical or generic was addressed by creating a tool that is easy to use and gives useful, personalized feedback based on self-reported answers.

The tool was trained with artificial input and tested by two actual organizations. One had no specialized IT personnel, and the business owner undertook the evaluation. The other had an IT manager who tested the tool. In both cases, a couple of employees also participated in the assessment process.

These tests helped ensure that the solution is usable by both technical and non-technical users, and that it provides value at different levels of the organization.

3.2 Questionnaire Design

One of the core contributions of this thesis was the development of two structured self-assessment questionnaires: one targeting organizational practices and another focusing on individual employee behavior. The goal was to maintain a balance between technical relevance and accessibility, allowing non-specialist users to self-assess meaningfully.

The process began with a review of well-established cybersecurity frameworks and guidelines, including the **NIST Cybersecurity Framework (CSF)** [29], **ISO/IEC 27001** [17], the Estonian **E-ITS framework** [19], and **ENISA's SME Guide** [30]. These sources provided domain structure and topic relevance, ensuring that the questionnaires addressed key aspects of cyber hygiene such as identity and access management, software updates, phishing awareness, backup and recovery, and remote work security.

However, most of the questions in these frameworks are designed for IT professionals or compliance officers, making them less accessible to non-technical users [1]. In developing the

questionnaires, care was taken to formulate questions that reflect the intent of established best practices while using simplified language and relatable terminology. This approach helps ensure that individuals without formal IT training can understand and answer meaningfully. For instance, instead of asking, "Does your organization enforce access control policies for administrative accounts?", the questionnaire uses phrasing like "Do you enforce multi-factor authentication (MFA) for all critical systems (e.g., email, financial systems, customer databases)?" Similarly, instead of broadly asking whether an "incident response framework" exists, the question becomes "Does your organization have a documented incident response plan?" with answer choices ranging from "No" to "Yes, regularly reviewed and tested."

Each question was structured with multiple-choice answers, graded from weak to strong cyber hygiene practices (on a scale from 0 to 4 points). The structured 0–4 scoring scale enabled automatic calculation of a total score, classification into risk levels, and generation of contextualized feedback.

The initial category structure was based on domains commonly emphasized in the reviewed frameworks, such as access control, software updates, and awareness training. Draft questions were tested using a set of example responses to check whether the categories provided balanced coverage and whether any questions overlapped in meaning or purpose. Based on these tests, some categories were adjusted and some questions were removed or reworded to reduce redundancy and improve clarity. The goal throughout was to keep the questionnaire concise and easy to complete, while still generating results detailed enough for meaningful feedback.

The final organizational questionnaire included **34 questions** across **11 categories**, while the employee questionnaire contained **17 questions** across **5 categories**. Each category containing between 1 to 6 questions. This scope was chosen to be as short as possible while still capturing meaningful data for personalized feedback generation. Overall, the design approach was guided by the principle of accessibility: to make cybersecurity self-evaluation possible without expert knowledge.

3.3 Web Interface

The web interface was manually designed and implemented to prioritize usability, accessibility, and simplicity, particularly for users without cybersecurity or technical experience. The goal was to build an intuitive and responsive front-end that works seamlessly across devices and screen sizes. TailwindCSS [31] was chosen for its utility-first styling approach, allowing consistent

layout and styling without complex Cascading Style Sheets (CSS) structures. JavaScript handled all dynamic behavior, including questionnaire rendering, progress tracking, user input handling, and feedback categorization, which was written and tested to ensure correct scoring and interaction flow.

To accelerate early prototyping, **DeepSite AI** [32] was used to generate an initial one-page Hypertext Markup Language (HTML) scaffold based on a written description of the desired layout. This prototype served only as a structural draft. The output was manually refactored into three modular files, `index.html`, `scripts.js`, and `styles.css`, to ensure maintainability, extensibility, and clarity of the codebase. The full prompt and AI-generated HTML are included in Appendix B.

GitHub Copilot [33] was also used throughout development, mainly for small code suggestions like HTML element scaffolding, common JavaScript patterns, and utility class combinations in TailwindCSS. However, all critical functionality, such as the frontend scoring logic, dynamic feedback rendering, and category breakdown logic, was written manually. Deliberate design and implementation decisions were made to ensure the application remained lightweight, privacy-preserving, and easy to deploy locally.

Unlike many tools that require external hosting or backend infrastructure, this tool comes with a built-in web server and can run entirely on the user's local computer. This approach was chosen to enhance privacy, reduce deployment friction, and make the tool accessible to any organization without the need for a hosted environment or advanced setup. It also allows the tool to work offline once launched, supporting broader usability in constrained or privacy-sensitive environments.

3.4 Scoring and Risk Classification

The scoring model was developed to convert questionnaire responses into standardized cyber hygiene scores. The goal was to make the results interpretable for nontechnical users while preserving enough detail to guide meaningful improvements.

How scoring works:

Each question in the assessment has multiple predefined answers, typically ranging from poor to strong cybersecurity practices. Each answer is assigned a numeric score between 0 (weakest practice) and 4 (best practice). When a user completes the questionnaire, their selected answers are collected, and a total score is computed relative to the maximum possible score.

To ensure fairness across varying questionnaire lengths and answer distributions, the total score is normalized into a percentage. The logic is as follows:

For each question:

- If the user has selected an answer, the associated score is added to the `total_score`.
- The maximum possible score for that question is determined by the number of answer options minus one (since scoring starts from 0).

Once all questions are processed:

- The final score is calculated as `(total_score / max_score) * 100`, resulting in a percentage value.
- If the maximum score is zero (e.g., in case of no questions), the function returns 0 to avoid division by zero.

This approach ensures that the final cyber hygiene score reflects relative performance, regardless of the number of questions or structure of the assessment.

Why this method:

The decision to base scoring on a simple percentage was made to ensure that the results are easy to communicate, visually representable (e.g., with progress bars), and comparable over time or between assessments. It avoids the complexity of weighted scoring or category-specific weighting, which could confuse end users and reduce transparency.

Risk classification:

Once the normalized percentage score is calculated, it is mapped to one of three risk levels:

- **High Risk:** 0–29%
- **Medium Risk:** 30–59%
- **Low Risk:** 60–100%

This tiered classification was chosen to reflect meaningful performance bands, where scores below 30% indicate serious gaps requiring urgent attention, 30–59% reflects partial implementation of good practices, and scores above 60% indicate relatively strong hygiene with room for improvement. It provides a qualitative summary of the user's security posture and serves as a basis for adjusting the tone and urgency of the generated feedback. For instance, a

low score results in more urgent language and critical recommendations, whereas a higher score prompts reinforcement of good practices and attention to remaining gaps.

Development and validation:

The scoring model was tested iteratively using simulated responses across different profiles — from minimal to ideal cybersecurity behaviors. This helped verify that the scoring output aligned with expected results and allowed fine-tuning of scoring thresholds and answer values where necessary.

The scoring function was designed to be technically simple, explainable, and consistent — providing a solid foundation for meaningful feedback while remaining fully transparent to the user.

3.5 AI-Powered Feedback Generation

A core feature of the Cyber Hygiene Feedback Tool is its ability to generate clear, personalized cybersecurity reports using generative AI. The purpose is to provide practical, human-readable feedback based on user responses — without requiring technical knowledge to interpret the results.

3.5.1 Data Processing and Prompt Construction

Before involving AI, the system first summarizes the self-assessment responses using a custom Python script. This includes:

- Identifying **strengths**: questions where the user's selected answer scored at least 3 points.
- Identifying **weaknesses**: answers with scores below 3, grouped by category.
- Calculating a total normalized score as a percentage.
- Assigning an urgency **tone** based on the score (e.g., *Critical*, *Improving*, *Strong*).

All of this information is assembled into a single structured text prompt that is passed to the AI model.

3.5.2 Feedback Prompt Structure

The prompt sent to the model follows a predefined format, ensuring consistency and completeness. It includes the following sections:

1. **Cyber Hygiene Score and Tone**

2. **Introduction**: A short summary of the current posture
3. **What You're Doing Well**: A bullet list of strengths
4. **Areas to Improve**: Grouped weaknesses by category
5. **Potential Risks and Risk Scenarios**: AI-generated based on findings
6. **Action Plan**:
    - Immediate (0–30 Days)
    - Short-Term (60–90 Days)
    - Medium-Term (3–6 Months)
7. **Conclusion**

This prompt is constructed using the user's score, strengths, and weaknesses. The complete prompt template is included in Appendix B.

AI Generation and Output Handling

Once the prompt is assembled, it is passed to OpenAI's GPT-4o model [6], which returns the final feedback text. This response is formatted and exported into a downloadable PDF using the `reportlab` [34] Python library.

Example

A typical input to the AI model might include a score (e.g 48.5%), strengths (e.g., encrypted communication, password manager use), and weaknesses (e.g., MFA not enforced, irregular training). Based on this, the AI generates a report with a tone (e.g "Critical: Your cyber hygiene practices need urgent improvement") and offers actionable next steps over three time horizons.

Full examples of these generated reports are provided in Appendix E.

Rationale

This approach allows the AI to reason holistically about the user's posture and generate rich, context-aware feedback that goes beyond static templates. By shifting responsibility for the full text structure to the AI rather than separating logic for risk extraction and action plan creation, the system reduces engineering complexity while maximizing flexibility and adaptability of the output.

3.6 Testing and Validation

Testing and validation of the system were conducted using both simulated data and real-world participants. The complete evaluation process and outcomes are described in detail in Section 6.

4. Design and Implementation of the Web Interface

The Cyber Hygiene Feedback Tool was built as a lightweight, browser-based web application designed to run locally. This approach minimizes deployment complexity, avoids external data transmission, and ensures privacy — especially important for organizations concerned about sharing internal cybersecurity practices online.

4.1 Setup and Deployment

The tool is distributed via a public GitHub repository[1]. To run the tool, users need to download the repository, insert their personal OpenAI API key into the configuration file (as explained in the README), and start a local server by running a Python script (e.g., `server.py`). The assessment interface then opens in a browser at `localhost:5000`.

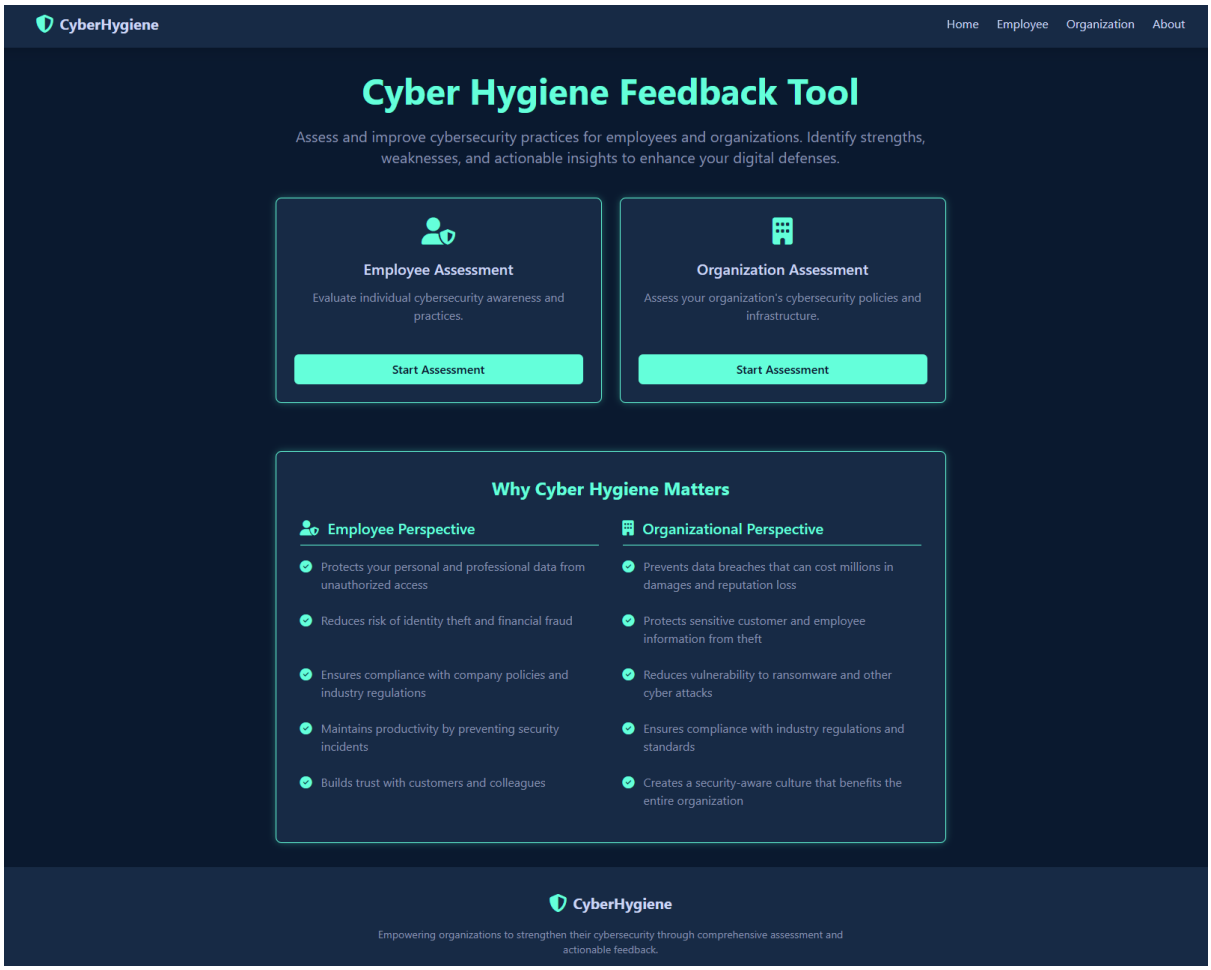

Figure 1. Homepage of the Cyber Hygiene Feedback Tool (local interface)

[1] https://github.com/MarcoKuusk/CyberHygieneFeedback

Integration with OpenAI:

To generate personalized feedback, the tool connects to OpenAI's GPT-4o model. Each user is required to create their own OpenAI account and insert their API key into a configuration file before using the tool. This setup process is documented in the repository's README[2] and is necessary for generating the downloadable AI-powered feedback reports. During validation, users successfully followed this process independently, demonstrating that the tool can be deployed without external assistance.

4.2 Architecture and Design Summary

The frontend was developed using HTML, JavaScript, and TailwindCSS. It handles questionnaire rendering, progress tracking, local scoring, and immediate feedback. The backend is powered by Flask [35] and is responsible for saving assessment data and calling the AI feedback generator, which returns a PDF report.

Key design decisions include:

- Keeping the full tool local — no user data is sent to external servers, except the anonymized prompt to OpenAI (only if the user generates a report).
- Structuring questions as JavaScript objects for easy editing.
- Providing both frontend feedback (static) and backend feedback (AI-generated PDF).

[2] https://github.com/MarcoKuusk/CyberHygieneFeedback/blob/main/README.md

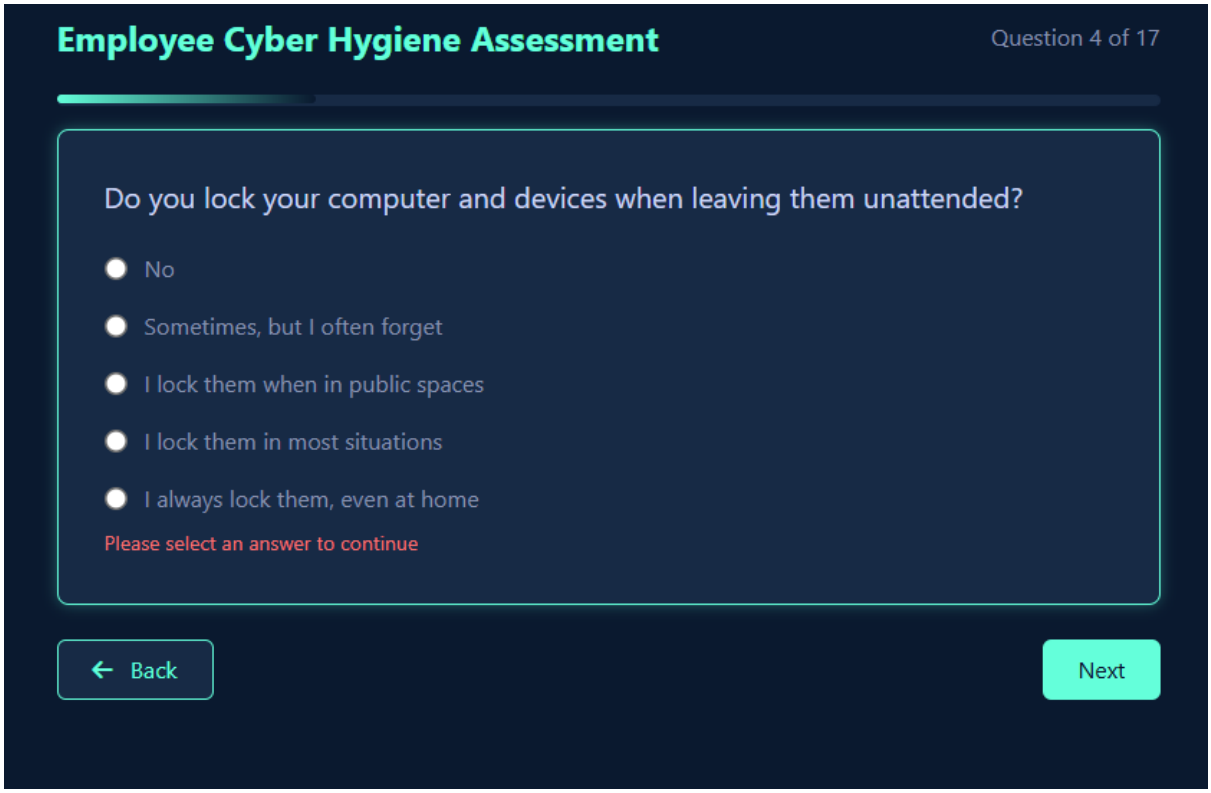

Figure 2. Assessment interface displaying one of the organization-level questions

Feedback is generated on the frontend using a predefined logic model embedded in the JavaScript code. Each question is linked to specific guidance for strengths and weaknesses depending on the score selected (0–4). These mappings are defined in a local data structure, which allows immediate classification of each response.

Figure 3. Frontend feedback view for an employee-level assessment

The separation of frontend logic (for interactive feedback) and backend logic (for comprehensive AI-generated reports) improves modularity. It ensures that users receive instant feedback without delay while still being able to download a more detailed PDF report powered by OpenAI's GPT-4o model [6].

Figure 4. Frontend feedback view for an organization-level assessment

This logic was also implemented to ensure that users receive actionable, categorized guidance instantly after assessment completion, without relying on the backend. It improves transparency and makes the tool useful even in offline or low-connectivity environments.

4.3 Simplified Deployment

No external hosting is required. The tool can be deployed by cloning the repository and running a Python server locally. While this requires basic technical familiarity, testing showed that even non-technical users could complete the setup using the README instructions.

5. Design and Implementation of the Automated Feedback

The automated feedback system is responsible for generating structured, personalized security guidance based on the results of the self-assessment questionnaire. It combines rule-based logic with OpenAI's GPT-4o [6] model to offer practical, understandable, and time-bound recommendations for both individual employees and organizations.

5.1 Why an Automated Approach Was Chosen

Manual cybersecurity reporting typically requires expert knowledge, time, and external resources. The aim of this tool was to create a scalable and accessible feedback system that organizations could use independently.

While rule-based systems can offer consistency and speed, they often produce rigid or generic advice [13, 14]. Generative AI, by contrast, enables dynamic, context-aware feedback using natural language [36]. By combining these approaches, the tool developed in this thesis generates personalized, actionable guidance without requiring in-house cybersecurity expertise or external consultants.

5.2 Architecture Overview

The feedback logic is implemented in Python and integrated into the backend using Flask. Two classes handle the main generation workflows:

- `EmployeeFeedbackGenerator`: Generates personalized feedback based on an employee's assessment responses.
- `OrganizationFeedbackGenerator`: Focuses on broader security processes and structural maturity.

Each class follows the same internal workflow: summarize findings, build an action plan, and generate a detailed PDF report using AI.

Each assessment submission is saved as a JavaScript Object Notation (JSON) file via the Flask backend. JSON was selected for its lightweight structure and compatibility with Python.

Feedback generation is triggered by a Flask backend endpoint, which runs the `main.py` script that handles the logic and calls the corresponding feedback class.

5.3 Feedback Generation Logic

Each generator class whether for the organizational or employee assessment follows a consistent, modular pipeline to transform assessment responses into structured, AI-generated feedback. The steps below explain in detail how each stage works and why it was designed that way.

5.3.1 Summarize Findings

Responses are first categorized based on their numeric score. Any answer that scores 3 or above is considered a strength, indicating that good practices are in place. Answers scoring below 3 are treated as weaknesses and grouped by thematic category (e.g., Passwords, Security Awareness & Training, Third-Party Risk). This threshold was chosen to clearly separate adequate practices from weaker ones. Grouping by category improves readability for the user and supports the prompt construction logic needed to generate meaningful feedback with the AI model.

5.3.2 Calculate Score

A total cyber hygiene score is calculated by dividing the user's total score by the maximum possible score and multiplying the result by 100. This creates a percentage-based score that is easily understood and allows for comparison over time or between assessments. The resulting score also supports classification into basic risk categories (e.g., High, Medium, Low), helping users understand their general posture at a glance.

5.3.3 Set Feedback Tone

Depending on the total score, the system selects a feedback tone — encouraging, moderate, or critical. This tone adjustment enhances the impact of the feedback by aligning the messaging with the user's performance level. It helps maintain user engagement while avoiding overly discouraging or overly reassuring language.

5.3.4 Generate Report

The constructed prompt is submitted to OpenAI's GPT-4o model, which returns a complete feedback report. The system then formats this into a downloadable PDF using a predefined layout. This format was chosen to ensure the report is easy to read, share, and revisit, making the feedback more useful in practice and over time.

5.4 Why GPT-4o Was Used

GPT-4o [6] was chosen for its ability to generate coherent, human-readable feedback from structured input [36]. The model can adjust its tone and detail level based on prompt design — critical for engaging non-technical users [36].

5.5 Why Feedback Is Not Shown Live in the Interface

The AI-generated report is long-form, detailed, and designed for formal review. Serving this content live would degrade the browser experience and delay response times. Instead, the web interface uses predefined logic embedded in each question to instantly display:

- **Strengths:** If the selected answer shows good practice.
- **Weaknesses:** If the selected answer reveals a gap.
- **Actionable Tip:** A direct, related recommendation.

This static feedback is rendered instantly in the browser, ensuring fast interaction. In contrast, the PDF report provides tailored, categorized, and concise feedback using AI.

Both feedback layers serve different purposes: fast learning via the UI, and deep analysis via downloadable reports.

5.6 Contributions and Tooling

All data processing, scoring logic, tone assignment, prompt engineering, and PDF formatting were implemented manually in Python. While GPT-4o generated the natural language content, the underlying architecture, data flow, and structural design were fully developed by the author.

6. Evaluation and Testing

This section evaluates the functionality, usability, and practical value of the Cyber Hygiene Feedback Tool through both simulated and real-world usage. The purpose of this testing phase was to ensure the system consistently generated accurate, actionable feedback for all users but also answer a central question:

Can this tool help non-technical users meaningfully assess and improve their cybersecurity posture without external support?

To answer this, both technical and practical tests were carried out across development stages.

6.1 Testing Methodology and Setup

Throughout development, the tool was tested using simulated data representing a variety of assessment scenarios. These tests aimed to verify the correctness of logic used for scoring, risk classification, action planning, and prompt generation. This internal validation helped uncover and fix issues in data handling, AI prompt formatting, and UI rendering early on.

Simulated assessments were saved in JSON format and processed using a local Flask backend, which mimicked actual usage conditions. Testing included responses with high, medium, and low scores to confirm that the output, both on the web interface and in the generated PDF, aligned with the intended logic.

End-to-end testing covered the full workflow: completing the questionnaire, triggering backend processing, and downloading the final AI-generated feedback report. These tests ensured that score calculations remained consistent between the frontend and backend, that data was interpreted correctly by the OpenAI's GPT-4o model, and that all outputs were presented in the correct format.

The goal of this phase was not to measure real-world behavioral change, but to verify that the tool works as designed and generates technically correct and logically consistent feedback across a range of expected user behaviors.

6.2 Real-World Usage: Organizational Testing

To evaluate the tool's practical value and real-world applicability, it was tested with two organizations based in Estonia: a cleaning services company and a non-profit operating in the mental health sector. These were selected through personal contacts to represent two different

operational and technical contexts. The cleaning company had no dedicated IT personnel, while the mental health organization employed a part-time IT manager. This allowed the tool to be tested across varying levels of digital literacy and internal technical support.

The solution was provided to both organizations via a GitHub repository that included the complete tool along with a README file containing installation instructions. As part of the setup, each organization was instructed to create an OpenAI account and insert their own API key into a designated configuration file. This step was required to enable the tool's AI-driven feedback generation and was successfully completed by both organizations without direct assistance, following the instructions in the repository.

Each organization downloaded the repository and installed the tool locally. The mental health organization completed setup independently using only the README file. The cleaning services company required more time due to unfamiliarity with GitHub but succeeded without direct intervention, demonstrating that the tool was accessible even for non-technical users.

Both organizations completed the full organization-level self-assessment using the web interface. The automatically generated PDF reports were reviewed in structured feedback sessions, where participants were asked to comment on the clarity, tone, and relevance of the recommendations.

Feedback was generally positive. Participants described the reports as "easy to follow" and "surprisingly detailed for something automated." One representative noted, "This gives us something concrete to work with — we now know exactly what to fix first." The other remarked that "The tone wasn't too technical but still serious enough to make us pay attention." These responses confirmed that the tool met its goal of providing accessible and actionable cybersecurity guidance.

The cleaning services organization performed a follow-up self-assessment approximately one week later after implementing several short-term recommendations. These included introducing basic internal security policies, deactivating unused accounts, creating backups, and limiting access rights for non-essential staff. Their cyber hygiene score rose from 13% to 26%, marking a 13-percentage point improvement.

Notably, the greatest progress was observed in the Identity and Access Management and Incident Response categories — areas where simple administrative changes could be made quickly. This case illustrates the tool's potential to support not just one-time evaluations but also continuous improvement through iterative use.

6.3 Real-World Usage: Employee Testing

Six individual users from different organizations and roles completed the employee-level cyber hygiene questionnaire. Most participants lacked formal cybersecurity training, providing a useful test case for evaluating whether the tool could support non-technical users.

All participants reported that the tool highlighted digital hygiene issues they were previously unaware of. The most common areas of concern were: (1) password reuse and poor password storage; (2) inconsistent screen locking habits; and (3) weak phishing awareness and link verification practices.

Three users performed a second self-assessment after taking small, corrective actions — such as enabling multi-factor authentication (MFA), using a password manager, and completing a short phishing awareness training. Their initial scores were 18.0%, 32.5%, and 37.0%, and their follow-up scores rose to 36.0%, 37.0%, and 40.3% respectively. This corresponds to individual improvements of 18.0, 4.5, and 3.3 percentage points, resulting in an average improvement of 9.6 percentage points across the three users.

The results suggest that the tool can help drive measurable behavior change, even with minimal intervention, and without requiring formal training. The follow-up scores and comments indicate that users were not only motivated to act but could also use the second evaluation as a form of feedback validation.

6.4 User Feedback and Observations

User perception played a central role in evaluating the tool's clarity, usefulness, and practicality. Feedback was collected through brief follow-up interviews after participants completed their respective assignments. These interviews were conducted either in person or via email, depending on participant availability. A total of eight individuals provided feedback: two representatives from the organizational-level testing and six employees from the employee-level assessment.

Most users emphasized that the AI-generated PDF reports were "easy to understand" and "written in a tone that doesn't feel robotic or overly technical." One employee commented, "I liked that it told me exactly what I'm doing right and what to fix — it didn't just give me a list of problems." Another mentioned that the phrasing "Always lock your screen, even at home" made the suggestion feel more like a habit-building tip than a technical instruction.

Users also responded positively to the browser-based feedback interface, particularly the clear sectioning of answers into "Strengths," "Areas to Improve," and "Risks." The visual feedback elements, such as color-coded bars showing overall scores or breakdowns by topic, were frequently cited as helpful. One organizational participant remarked, "The visual layout makes it much easier to explain the results to our team."

Specific suggestions for improvement included:

- **Adding examples for certain items.** For example, instead of only saying "Encrypt sensitive files," one user proposed including an example such as: "Use free tools like 7-Zip with password protection or built-in encryption in Office 365."
- **A request for multilingual support,** particularly Estonian, Russian, and Finnish. A participant from a non-profit organization noted that "some of our staff would benefit more if the tool was available in their first language."
- **An additional feature for saving progress and resuming later,** especially for longer questionnaires. One participant working in a managerial role commented, "I had to pause halfway through and re-enter my answers later. A save button would help."

These comments were used to fine-tune both the language in the OpenAI GPT-4o prompt and the frontend structure. The feedback prompt was updated to include more real-world phrasing and context, and the frontend elements were reorganized for improved readability, especially on smaller screens.

6.5 Limitations

While the testing and validation process provided valuable insights into the usability and effectiveness of the tool, several limitations should be acknowledged.

First, the scope of real-world validation was limited to two organizations and eight individual users, all based in Estonia and approached through personal contacts. While these participants represented different sectors and technical backgrounds, the small sample size and informal recruitment process limit the generalizability of the findings. Broader testing across diverse sectors, geographic regions, and user types would be necessary to draw more robust conclusions about the tool's effectiveness in varied organizational contexts.

Second, the validation focused primarily on short-term feedback and impressions gathered shortly after users completed the assessments. While some participants conducted a follow-up

evaluation after taking action, this timeframe was limited to a few days or weeks. Longer-term studies would be required to assess whether the tool drives sustained changes in behavior or policy, and whether repeated use can support continuous improvement.

Third, although the tool was distributed through a public GitHub repository, users were required to configure it independently and obtain their own OpenAI API key to enable feedback generation. While this requirement was met successfully by all test participants, it may pose a barrier for some future users unfamiliar with API services. Simplifying this step or offering integrated key management could improve accessibility.

Finally, while the AI-generated feedback was generally well-received, it is important to note that the responses from the GPT-4o model are not fully deterministic. The same input may produce slightly different outputs depending on model behavior and versioning. Although the prompt structure was designed to reduce this variability, it remains a known limitation of using generative AI for consistent reporting. Future work could explore techniques such as priming the model with structured background knowledge or using fine-tuned models to enhance output stability and domain specificity.

Overall, while the initial evaluation supports the tool's value and usability, further testing at scale and over longer periods is recommended to fully validate its impact and refine its deployment model.

7. Discussion and Conclusion

This section reflects on the performance, usability, and design trade-offs of the Cyber Hygiene Feedback Tool. It discusses how the tool met its goals, the value it delivered in testing, and outlines possible directions for future work.

Key Observations

The tool proved effective in generating structured and personalized cybersecurity feedback, both at the organizational and individual levels. It delivered recommendations that users found relevant and understandable — a common weakness in many existing tools. By integrating OpenAI's GPT-4o model, the system provided scenario-based advice that responded directly to specific weaknesses instead of offering only generic best practices.

In real-world usage, improvements were measurable. One organization increased its cyber hygiene score from 13% to 26% by implementing basic practices such as internal policy documentation and account cleanup. Similarly, employees who re-tested after making changes, such as enabling multi-factor authentication or using password managers, saw an average improvement of 9.6 percentage points. While the sample size was small and informally recruited, these results suggest that clear, personalized feedback can drive meaningful behavior change with minimal overhead.

It is important to emphasize that this tool is not a replacement for professional cybersecurity audits or compliance frameworks [4]. Rather, it serves as a lightweight, preparatory mechanism — helping users understand their current risks and prioritize concrete improvements. The goal is to raise awareness and lower the entry barrier for organizations that lack access to specialized security expertise.

Future Directions

Although the tool met its primary goals, several areas for future development were identified through testing, participant feedback, and critical reflection.

Adaptive questionnaires. Currently, both the organizational and employee questionnaires are static — all users receive the same set of questions regardless of their responses or sector. A future version could introduce adaptive questionnaires that tailor follow-up questions based on earlier answers (e.g., skipping MFA-related questions if MFA is already implemented) or user

type (e.g., focusing more on data privacy in the healthcare sector). This could shorten the time required to complete the assessment while increasing relevance and engagement.

Extending questionnaires. A larger question pool could theoretically provide more thorough coverage of cyber hygiene practices. However, based on framework alignment and initial validation, the current questions already cover the most critical domains identified in NIST CSF, ISO/IEC 27001, ENISA SME Guide, and E-ITS. While adding more questions might slightly improve precision, it is unlikely to substantially enhance feedback accuracy unless combined with an adaptive or risk-prioritized structure. The trade-off between thoroughness and usability must also be considered — longer questionnaires may reduce user completion rates. Therefore, future work should focus not only on expanding the question bank but also on intelligently selecting which questions to ask in each context.

Offline feedback generation. At present, the tool relies on OpenAI's GPT-4o API to generate its reports. While no sensitive data is transmitted, there are concerns about external dependencies and data privacy. Future versions could explore the use of offline-compatible language models (e.g., open-source LLMs running locally) to provide full functionality without requiring internet access. This would make the tool more suitable for environments with strict compliance or data residency requirements.

Multi-language support. Multiple participants noted that availability in additional languages would increase accessibility, particularly for organizations in Estonia where staff members may prefer to interact with the system in Estonian or Russian. Offering both the questionnaire and generated feedback in multiple languages would improve usability across broader demographics and sectors.

Score tracking and progress over time. While the current version generates feedback for each assessment instance, it does not track user progress over time. A simple, privacy-preserving storage mechanism could allow users to view trends across multiple assessments, compare scores before and after interventions, and evaluate the long-term impact of their improvements. This feature could add significant value for organizations seeking continuous security improvement rather than one-time audits.

Gamification and motivation. Participants appreciated the clarity and structure of the feedback, but some suggested integrating motivational elements — such as badges for completing certain sections, highlighting areas of improvement, or offering practical challenges ("Improve your

phishing awareness score this month"). These elements could enhance engagement, especially for repeat users at the employee level.

Save-and-continue functionality. Some users, particularly on the organizational side, suggested that the assessment might be too long to complete in one sitting. A "Save Progress" or "Resume Later" feature would improve usability for busy users and support more flexible usage in real-world settings.

More contextual examples in action plans. Several users requested that the AI-generated action plans include more concrete, tool-specific examples. For example, instead of recommending "Establish device encryption," the feedback could mention tools like BitLocker, FileVault, or mobile device management solutions. Including such references would make it easier for users to act on recommendations without additional research or consulting.

Conclusion

This thesis set out to create a practical, accessible cybersecurity self-assessment and feedback system for organizations in varying sizes. By combining rule-based scoring, natural language generation, and a user-friendly interface, the Cyber Hygiene Feedback Tool successfully delivered personalized, non-technical guidance to real users.

The evaluation, through both simulations and real-world testing, confirmed that the tool is usable without external support and can motivate concrete improvements in cyber hygiene. The modular architecture also ensures maintainability, adaptability, and transparency of logic, enabling future development or customization.

The strength of this work lies not in technological novelty, but in the careful integration of existing technologies into a useful and scalable solution. It fills a gap between lightweight awareness platforms and expert-driven audit tools, offering meaningful feedback in a format that non-specialists can act on.

In its current form, the tool already adds value to cybersecurity education and risk reduction for organizations. With further refinement and testing, it has the potential to scale into a widely usable framework for early-stage cybersecurity self-improvement.

References

[1] Junior C. R., Becker I., and Johnson S. Unaware, Unfunded and Uneducated: A Systematic Review of SME Cybersecurity. *arXiv* (2023). https://arxiv.org/pdf/2309.17186.

[2] Erdogan G., Halvorsrud R., Pickering B., and Boletisis C. Cybersecurity Awareness and Capacities of SMEs. *ResearchGate* (2023). https://www.researchgate.net/publication/367253444_Cybersecurity_Awareness_and_Capacities_of_SMEs.

[3] Curtin M., Melanie Gruben B. S. nad, Kozma N., O'Carroll G., and Murray H. Development of a cyber risk assessment tool for Irish small business owners. *arXiv preprint arXiv:2408.16124* (2024). https://arxiv.org/pdf/2408.16124.

[4] Rahman M. M., Kshetri N., Abu S. A. S., and Rana M. M. AssessITS: Integrating procedural guidelines and practical evaluation metrics for organizational IT and Cybersecurity risk assessment. *arXiv preprint arXiv:2410.01750* (2024). https://www.researchgate.net/publication/384599117_AssessITS_Integrating_procedural_guidelines_and_practical_evaluation_metrics_for_organizational_IT_and_Cybersecurity_risk_assessment.

[5] Leszczyna R. Review of cybersecurity assessment methods: Applicability perspective. *Computers Security* 108 (2021), p. 102376. DOI: https://doi.org/10.1016/j.cose.2021.102376. https://www.sciencedirect.com/science/article/pii/S0167404821002005.

[6] OpenAI. GPT-4o. 2024. https://openai.com/index/hello-gpt-4o/ (05/15/2025).

[7] Ejjami R. Enhancing Cybersecurity through Artificial Intelligence: Techniques, Applications, and Future Perspectives. *Journal of Next-Generation Research* (2024). https://www.researchgate.net/publication/385872905_Enhancing_Cybersecurity_through_Artificial_Intelligence_Techniques_Applications_and_Future_Perspectives.

[8] Ahmed S., Rahman A. B. M. M., Alam M. M., and Sajid M. S. I. SPADE: Enhancing Adaptive Cyber Deception Strategies with Generative AI and Structured Prompt Engineering. 2025. https://arxiv.org/pdf/2501.00940.

[9] Shojaifar A., Fricker S. A., and Gwerder M. Automating the Communication of Cybersecurity Knowledge: Multi-Case Study. *arXiv preprint arXiv:2007.07602* (2020). https://arxiv.org/pdf/2007.07602.

[10] Qawasmeh S. A.-D., AlQahtani A. A. S., and Khan M. K. Navigating Cybersecurity Training: A Comprehensive Review. *arXiv preprint arXiv:2401.11326* (2024). https://arxiv.org/abs/2401.11326.

[11] European Union Agency for Cybersecurity (ENISA). Cybersecurity Maturity Assessment for Small and Medium Enterprises. 2023. https://www.enisa.europa.eu/tools/cybersecurity-maturity-assessment-for-small-and-medium-enterprises (05/15/2025).

[12] Cyber Readiness Institute. Cyber Readiness Institute. 2025. https://cyberreadinessinstitute.org/ (05/15/2025).

[13] Kwasny S. C. and Faisal K. A. Overcoming limitations of rule-based systems: An example of a hybrid deterministic parser. *Proceedings of the International Conference on Intelligent Systems and Knowledge Engineering*. ResearchGate, 2014. https://www.researchgate.net/publication/221449280_Overcoming_Limitations_of_Rule-Based_Systems_An_Example_of_a_Hybrid_Deterministic_Parser.

[14] Heckerman D. and Horvitz E. J. The Myth of Modularity in Rule-Based Systems. *arXiv preprint arXiv:1304.3090* (2013). https://arxiv.org/abs/1304.3090.

[15] Chen B., Zhang Z., Langrene N., and Zhu S. Unleashing the potential of prompt engineering for large language models. *ScienceDirect* (2025). https://www.sciencedirect.com/science/article/pii/S2666389925001084.

[16] Standards N. I. of and Technology. The NIST Cybersecurity Framework (CSF) 2.0. 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf (05/15/2025).

[17] Standardization I. O. for. ISO/IEC 27001:2022 - Information security, cybersecurity and privacy protection — Information security management systems — Requirements. 2022. https://www.iso.org/standard/27001 (05/15/2025).

[18] Systemi. Overcoming Common ISO 27001 Challenges for Small Companies. *Systemi* (2025). https://systemi.se/2025/01/19/iso-27001-challenges-for-small-companies/ (05/15/2025).

[19] Riigi Infosüsteemi Amet (RIA). Eesti infoturbestandard (E-ITS). 2023. https://eits.ria.ee (05/15/2025).

[20] Stoltz M. The Road to Compliance: Executive Federal Agencies and the NIST Risk Management Framework. *arXiv preprint arXiv:2405.07094* (2024). https://arxiv.org/abs/2405.07094.

[21] CybExer. Kybertest - Cyber Security Awareness Test. 2025. https://www.kybertest.ee/ (05/15/2025).

[22] CybExer. Digiriigi Akadeemia - Cyber Hygiene Course. 2025. https://digiriigiakadeemia.ee (05/15/2025).

[23] Cybexer. MyCyberHygiene.com. 2025. mycyberhygiene.com (05/15/2025).

[24] CybExer. CybExer Cyber Range Technology. 2025. https://cybexer.com/cyber-range-technology (05/15/2025).

[25] Technologies C. Cyber Hygiene UT. 2025. https://cyberhygiene.ut.ee/ (05/15/2025).

[26] National Cyber Security Centre. What is the Cyber Essentials Readiness Tool? 2023. https://www.ncsc.gov.uk/files/Cyber-Essentials-Readiness-Tool-Leaflet.pdf (05/15/2025).

[27] University of Tartu, NCSC-EE. Organisation's information security maturity level evaluation. Accessed: 2025-01-21. 2025. https://mass.cloud.ut.ee/test-massui/#/ (01/21/2025).

[28] Hevner A. R., Ram S., March S. T., and Park J. Design science in information systems research. *MIS quarterly* (2004). https://www.researchgate.net/publication/201168946_Design_Science_in_Information_Systems_Research.

[29] National Institute of Standards and Technology. Cybersecurity Framework. 2024. https://www.nist.gov/cyberframework (05/15/2025).

[30] ENISA. Cybersecurity Guide for SMEs - 12 Steps to Securing Your Business. 2021. https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes (05/15/2025).

[31] Kombai. Tailwind CSS. 2025. https://tailwindcss.com (05/15/2025).

[32] AI D. DeepSeek Developer Tools and Template Generation. 2025. https://enzostvs-deepsite.hf.space (05/15/2025).

[33] GitHub. GitHub Copilot: Your AI pair programmer. 2024. https://github.com/features/copilot (05/15/2025).

[34] Robinson A., Becker R., ReportLab team the, and community the. ReportLab Toolkit. Version 4.4.0. Accessed: 2025-05-14. 2025. https://www.reportlab.com/ (05/15/2025).

[35] Projects P. Flask. 2025. https://palletsprojects.com/p/flask/ (05/15/2025).

[36] Bubaš G. The use of GPT-4o and other large language models for the improvement and design of self-assessment scales for measurement of interpersonal communication skills. *arXiv preprint arXiv:2409.14050* (2024). https://arxiv.org/abs/2409.14050.

Appendices

A. Self-Assessment Questionnaires

The Self-Assessment Questionnaires for both Organizations and Employees can be found in the dedicated GitHub repository:
https://github.com/MarcoKuusk/CyberHygieneFeedback/tree/main/Self-Assessment_Questionnaires

B. AI Prompt Example Sent to ChatGPT (GPT-4o)

The exact input prompt and corresponding generated feedback report can be found in the dedicated GitHub repository:

https://github.com/MarcoKuusk/CyberHygieneFeedback/tree/main/PromptExample

C. Developing the Base for the Web Interface with the Use of DeepSite AI

The interaction with DeepSite AI can be found in the dedicated GitHub repository: https://github.com/MarcoKuusk/CyberHygieneFeedback/blob/main/AI_Diaries/DeepSite_AI/DeepSite_AI.pdf

D. Example Interaction with Copilot

An example interaction with Copilot AI can be found in the dedicated GitHub repository: https://github.com/MarcoKuusk/CyberHygieneFeedback/blob/main/AI_Diaries/CoPilot/CoPilotAI.pdf

E. Example Feedback Reports

More example feedback reports for both web interface and PDF can be found in the dedicated GitHub repository:

https://github.com/MarcoKuusk/CyberHygieneFeedback/tree/main/Example_Reports

F. Full Example Feedback Report (Organization-Level)

The following is a full example of an automatically generated PDF report produced by the tool, based on organization-level responses. It illustrates the format, tone, and content structure that users receive after completing the assessment.

Organization Feedback

Cyber Hygiene Score

13.24%

Severe: Immediate and decisive cybersecurity action is required.

Introduction

The current cybersecurity hygiene of your organization is weak. With a Cyber Hygiene Score of 13.24%, it is vital to recognize the need for urgent improvements. Cyber threats are evolving, and safeguarding your business's data and operations requires ongoing effort. Prioritizing cybersecurity enhancements will help protect your assets and maintain trust with your clients and partners.

What You're Doing Well

Here are some areas where your organization is doing well:

- **Operating Systems, Software, and Applications Updates**:

Regular updates help patch known vulnerabilities, preventing attacks exploiting outdated software.

- **Data Backups**:

Frequent data backups ensure that you can quickly recover important information in the event of data loss or a cybersecurity incident.

Areas to Improve

Below are areas that need improvement, categorized for clarity:

Identity & Access Management

- **Multi-Factor Authentication (MFA)**: Implement MFA to protect critical systems against unauthorized access.
- **User Access Privileges**: Regularly review access privileges to prevent unauthorized data access.
- **Password Policies**: Enforce strong password rules to strengthen account security.
- **Employee Account Deactivation**: Immediately deactivate accounts of inactive or terminated employees to prevent misuse.

- **Least Privilege Principle**: Limit data access based on employee roles to minimize potential breaches.
- **Password Managers**: Educate employees on using password managers to secure credentials efficiently.

Software & Patch Management

- **Centralized Software Updates**: Establish a centralized system to ensure timely software updates.
- **Vulnerability Scans**: Conduct regular scans to identify and address security vulnerabilities.
- **Antivirus Solutions**: Deploy and update comprehensive antivirus and endpoint solutions to prevent malware infections.

Data Classification & Protection

- **Data Classification Policy**: Implement a formal policy to manage sensitive data access.
- **Data Encryption**: Encrypt sensitive files in transit and at rest to protect against unauthorized access.

Backup & Recovery

- **Backup Process**: Develop a robust data backup and recovery process.
- **Secure Backup Storage**: Ensure backups are stored securely offsite or in the cloud.
- **Backup Testing**: Regularly test backups to ensure data can be restored successfully.

Security Awareness & Training

- **Cybersecurity Training**: Provide regular cybersecurity awareness training to all employees.
- **Simulated Phishing**: Conduct tests to improve employee vigilance against phishing attacks.
- **Role-Specific Training**: Offer training tailored to specific job responsibilities.
- **Incident Reporting**: Educate employees on reporting security incidents and suspicions.

Network & Endpoint Security

- **Wi-Fi Security**: Implement secure Wi-Fi policies, including guest network separation.
- **Endpoint Protection**: Ensure all devices have updated security solutions to detect threats.
- **Remote Access Security**: Secure how employees access company data remotely, such as by using VPNs.

Incident Response & Business Continuity

- **Incident Response Plan**: Create a documented plan for responding to cybersecurity incidents.
- **Cybersecurity Support**: Establish relationships with experts to assist during emergencies.
- **Incident Analysis**: Analyze logged incidents for patterns to prevent future occurrences.
- **Cyber Insurance**: Consider cyber insurance to reduce financial losses from incidents.

Compliance & Regulatory Alignment

- **Regulations & Standards**: Align your practices with industry-specific cybersecurity regulations.
- **Vendor Standards**: Require third-party vendors to follow your cybersecurity standards.

Physical Security

- **Device Security**: Ensure physical security measures are in place for critical equipment.

Third-Party Risk

- **Vendor Assessment**: Evaluate the cybersecurity of vendors before sharing data.

Remote Work Security

- **Secure Networks**: Mandate VPNs or secure networks for remote work access.

Potential Risks and Risk Scenarios

Without improvements, specific risks include:

- An attacker taking control of email accounts due to the lack of MFA.
- Data breaches from excessive user privileges remaining unreviewed.
- Malware infections from outdated software, risking operation disruptions.

Action Plan

Immediate (0–30 Days)

- Implement MFA for all critical systems.
- Enforce strong password policies, including the use of password managers.
- Set up centralized software update management.
- Conduct vulnerability scans and update antivirus solutions.
- Establish secure remote access protocols via VPNs for remote work.

Short-Term (60–90 Days)

- Review and adjust user access privileges following the least privilege principle.
- Train employees on cybersecurity awareness and incident reporting.
- Identify and encrypt sensitive files and communications.
- Initiate regular backup testing procedures.
- Develop a documented incident response plan.

Medium-Term (3–6 Months)

- Formalize a data classification policy and conduct an inventory of sensitive data.
- Align cybersecurity practices with industry regulations and standards.
- Conduct simulated phishing attacks to enhance employee awareness.
- Evaluate third-party vendors for their cybersecurity practices.
- Consider implementing a cyber insurance policy for risk mitigation.

Conclusion

Continuously improving your cybersecurity strategy is essential. I recommend reassessing your security posture in 6–12 months. Remember, even small steps can significantly lower your risks and protect your organization's valuable data and reputation.

License

Non-exclusive licence to reproduce the thesis and make the thesis public

I, **Marco Kuusk**,

1. grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the digital archives of the University of Tartu until the expiry of the term of copyright, my thesis **Cyber Hygiene Feedback Tool**, supervised by **Arnis Paršovs**;
2. grant the University of Tartu a permit to make the thesis specified in point 1 available to the public via the web environment of the University of Tartu, including via the digital archives, under the Creative Commons licence CC BY NC ND 4.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright;
3. am aware of the fact that the author retains the rights specified in points 1 and 2;
4. confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Marco Kuusk,
13.05.2025