Kaunas University of Technology

PR00B251 Product Development Project

Cybersecurity Assessment Service

Intermediate Report

Prepared by K553 team:

Stanislav Puida, V BSen-2
Damla Goztas, SM-3/3
Deimantė Laureckytė, SM-3/3

Mentor:

Jr. Assist. Prof. Beldyga Natalia Ewa

Kaunas, 2025

Kaunas University of Technology

Stanislav Puida

Damla Goztas

Deimantė Laureckytė

Cybersecurity Assessment Service

Declaration of Academic Integrity

I confirm the following:

1. I have prepared the product development project independently and honestly without any violations of the copyrights or other rights of others, following the provisions of the Law on Copyrights and Related Rights of the Republic of Lithuania, the Regulations on the Management and Transfer of Intellectual Property of Kaunas University of Technology (hereinafter – University) and the ethical requirements stipulated by the Code of Academic Ethics of the University;

2. All the data and research results provided in the project are correct and obtained legally; none of the parts of this project are plagiarised from any printed or electronic sources; all the quotations and references provided in the text of the final degree project are indicated in the list of references;

3. I have not paid anyone any monetary funds for the product development project or the parts thereof unless required by the law;

4. I understand that in the case of any discovery of the fact of dishonesty or violation of any rights of others, the academic penalties will be imposed on me under the procedure applied at the University; I will be expelled from the University and my project can be submitted to the Office of the Ombudsperson for Academic Ethics and Procedures in the examination of a possible violation of academic ethics.

Stanislav Puida
Damla Goztas
Deimantė Laureckytė

Confirmed electronically

Table of Contents

List of figures

List of tables

List of abbreviations and terms

Abbreviations:

Assoc. Prof. – associate professor;

Jr. Assist. Prof. – junior assistant professor;

Lect. – lecturer;

Prof. – professor.

Terms:

Simulated Cyber Attacks – Controlled phishing, social engineering, and penetration testing to evaluate an organization's security posture.

V**ulnerability Reports** – Detailed insights on security weaknesses, potential risks, and recommendations for improvement.

Cyber Awareness Training – Educational courses and workshops to train employees on recognizing and mitigating cyber threats.

Introduction

Businesses are becoming increasingly concerned about cyber attacks because they run the danger of suffering monetary losses, data breaches, and harm to their brand. Many businesses are not prepared or informed enough to stop cyberattacks. Our initiative tackles this issue by offering comprehensive reporting, awareness training, and controlled cybersecurity testing, including phishing simulations and vulnerability assessments, to increase corporate resilience against actual cyberthreats.

Aim and objectives

The aim is creating a cybersecurity service that simulates controlled cyberattacks on companies, evaluates their vulnerabilities, and offers practical suggestions to improve security and cyber awareness is the goal of this project. An enhancement in the cybersecurity posture and threat recognition and response capabilities of clients is an outcome we seek.

To achieve this aim, the following objectives are set:

1. **Develop a cybersecurity testing service** that includes controlled phishing campaigns, penetration testing, and social engineering simulations tailored to client needs.
2. **Develop and implement a reporting** system that offers businesses a comprehensive understanding of their security vulnerabilities, attack success rates, and suggestions for enhancement.
3. **Develop a cyber awareness training program** that is tailored to the results of the test in order to provide employees with the necessary knowledge to identify and prevent cyber threats.
4. **Ensure compliance with cybersecurity standards and regulations** to align with best practices and legal requirements for ethical security testing.
5. **Assess the effectiveness of the service** by measuring improvements in clients' security awareness and response capabilities over time.

Each objective will be analyzed at the end of the project to extract key insights and ensure continuous improvement of the service.

Structure of the report

The report is arranged in a clear and systematic way. Firstly, it starts with an introduction that gives a summary of the cybersecurity assessment service. This followed by sections that shows the assessment methodology, detailing the steps performed to evaluate cybersecurity risks. The report then delivers the findings, significant security vulnerabilities and areas that raise concern. It also offers suggestions for enhancing cybersecurity, detailing specific aims and objectives to reduce risks. Lastly, the report wraps up with a recap of the assessment and any subsequent actions. Additional information may be found in appendices.

Team

Table 1 provides the team composition: students, their academic groups and titles of the study programmes.

Table **1**. Members of Product development project K553 team

Name Surname	Academic group	Study programme
Stanislav Puida	V BSen-2	Business Digitalization Management
Damla Goztas	SM-3/3	Communication Studies and Information Management Technologies
Deimantė Laureckytė	SM-3/3	Communication Studies and Information Management Technologies

1. Product Idea and Preparation

Businesses are becoming increasingly concerned about cyber attacks because they run the danger of suffering monetary losses, data breaches, and harm to their brand. Our initiative tackles this issue by offering comprehensive reporting, awareness training, and controlled cybersecurity testing, including phishing simulations and vulnerability assessments, to increase corporate resilience against actual cyberthreats.

1.1. Product idea

Our mentor, Jr. Assistant Professor Beldyga Natalia Ewa, gave the suggestion to team K553 which was originally denominated "Preparedness, Resilience, and Response Capacity of the Civilian Population to Crisis and Emergency". With this premise, we honed our area of expertise into the research question of "How could we assist university students and staff to engage immediately in the event of a cyberattack on the university information system, while protecting data and ensuring business continuity?"

At first, we thought a real-time warning assistant for cybersecurity would be a good proposal, capable of identifying a threat, guiding the individuals through the steps of responding, while educating the individual about safe digital practices. But by week 5, when we started to market research, we saw that our solution would need to economically sustainable. This led us to restate the initiative as a cybersecurity risk assessment service for businesses.

Thus, our project is a cybersecurity vulnerability assessment service that enables businesses to identify vulnerabilities through simulated cyberattacks, which includes actionable recommendations for improved security. The service includes:

1. Simulated Cyber Attacks – Performing controlled phishing attacks, penetration testing and vulnerability assessments to uncover security vulnerabilities.

2. Security Reporting – Providing businesses with extensive reporting and recommendations to improve their cybersecurity practices.

3. Cyber Awareness Training – Offering educational courses and workshops to help employees recognize and prevent cyber threats.

The goal is to enhance cybersecurity awareness and resilience among businesses by identifying risks before real attackers exploit them. The service is targeted at companies that want to test their security measures, educate employees, and comply with industry security standards.

On the attached figures 1 our webpage mockup could be seen. The main page will show “Dashboard” with the plot of finished simulated phishing for example. Then, there are few pie charts like: “Email sent”, “Email Opened”, “Clicked Link” and “Submitted Data” which are pretty self explanatory. Next there will be a list of “Recent Campaigns”.

On Figure 2 would be seen more detailed results of selected campaign.

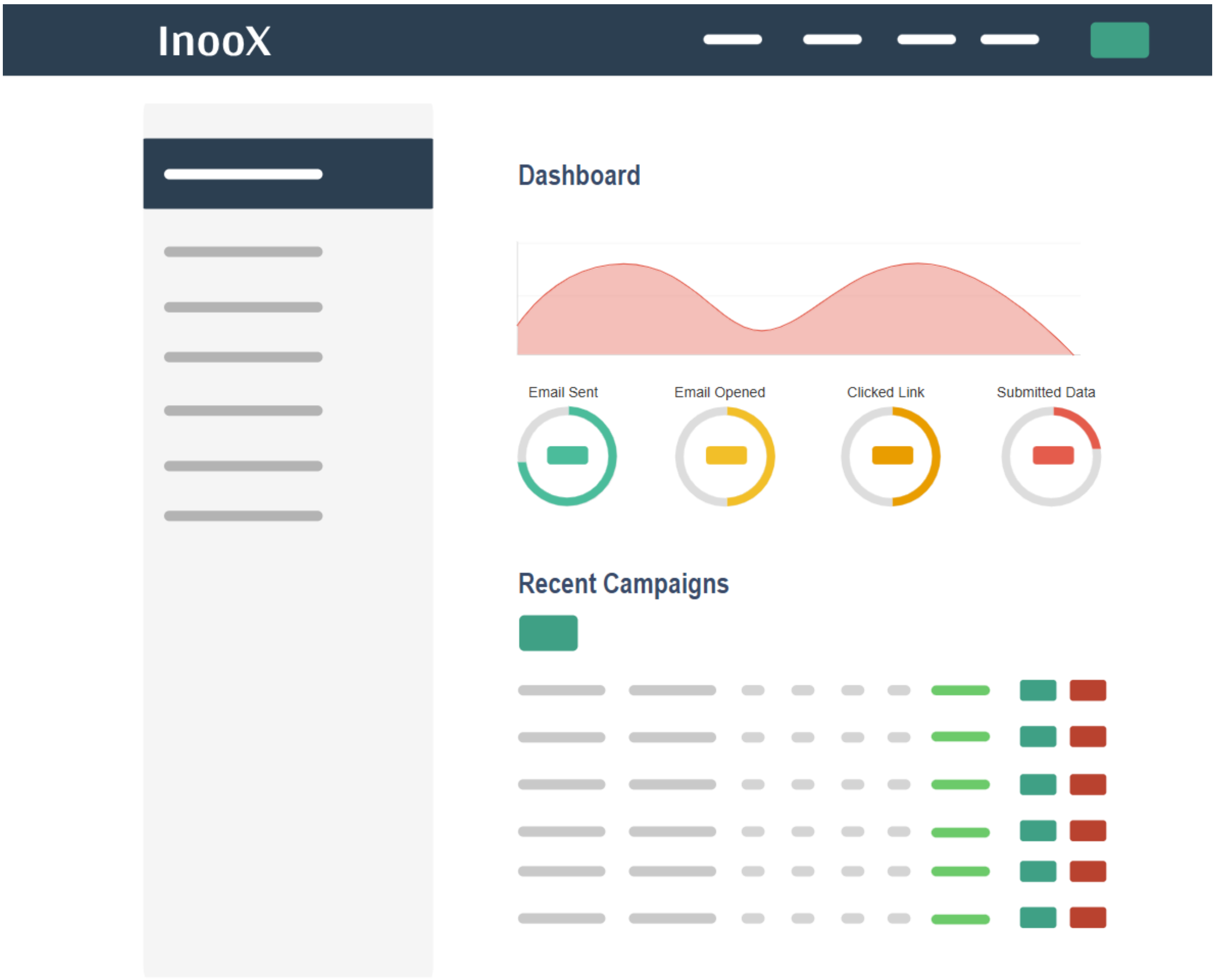


Fig. 1. Screenshot of mock-up of product webpage with core features user will be able to see

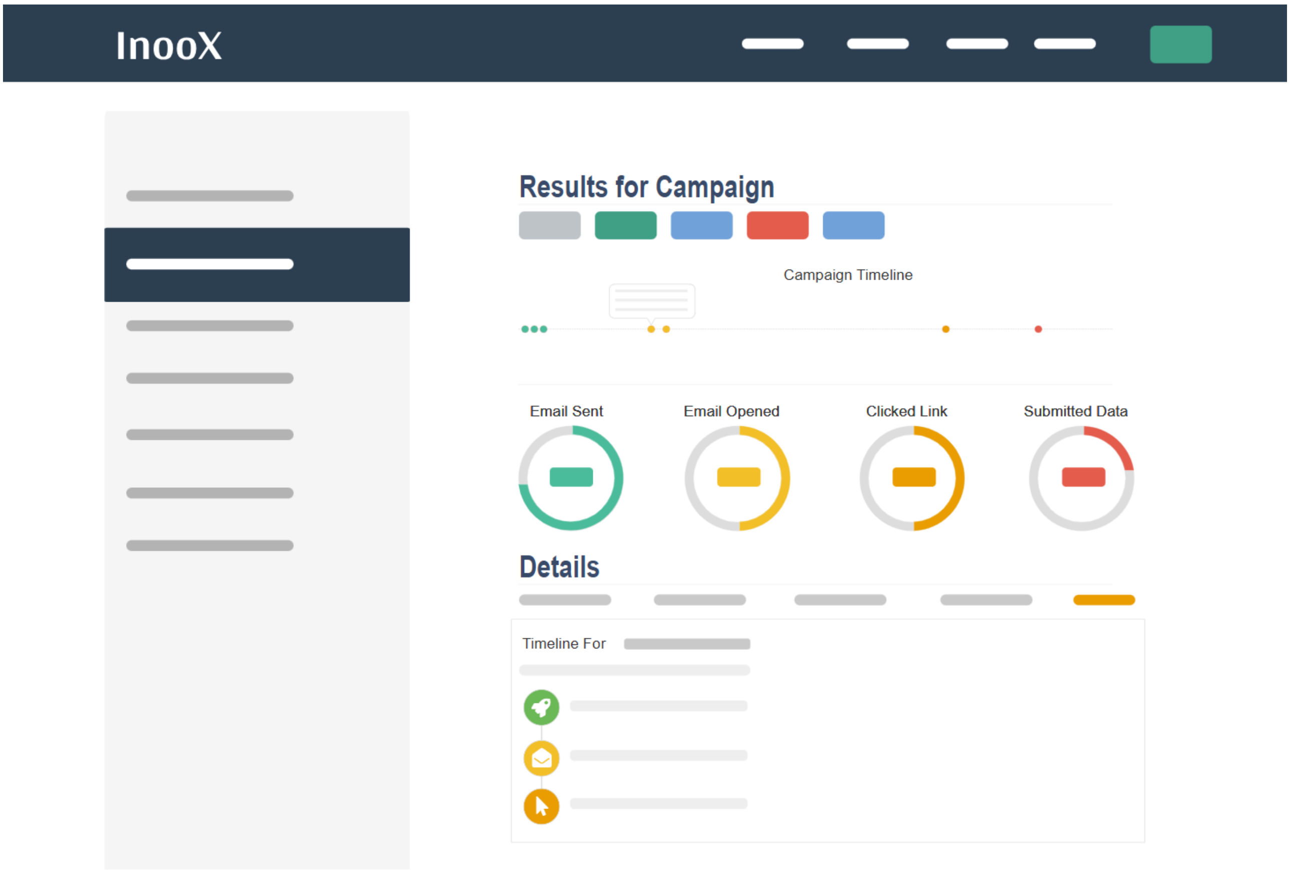


Fig. 2. Screenshot of mock-up of product webpage with core features user will be able to see

The included figures demonstrate a potential web-based interface to track phishing simulation campaigns. Figure 1 depicts an overall dashboard used to visualize key performance indicators relevant to simulated phishing attempts. There are visual data displays showing the user engagement indicators and the outcomes of the campaigns, all in support of assessing overall security awareness levels. A summary of past campaigns also appears to ease access to ongoing past/present simulations. Figure 2 outlines more detailed reporting methodologies for each campaign, allowing an analysis of the individual campaign results. This reporting format will allow the organizations to maintain tracking of the progress of their cyber training activities and enhance its effectiveness.

1.2 Product Development Method

To bring our cybersecurity assessment service to life, we followed the design thinking approach – a flexible, user-focused method that helped us better understand our potential clients and build a solution around their real needs. This process guided us trough several stages: empathizing with users, defining the problem, brainstorming ideas, prototyping and testing.

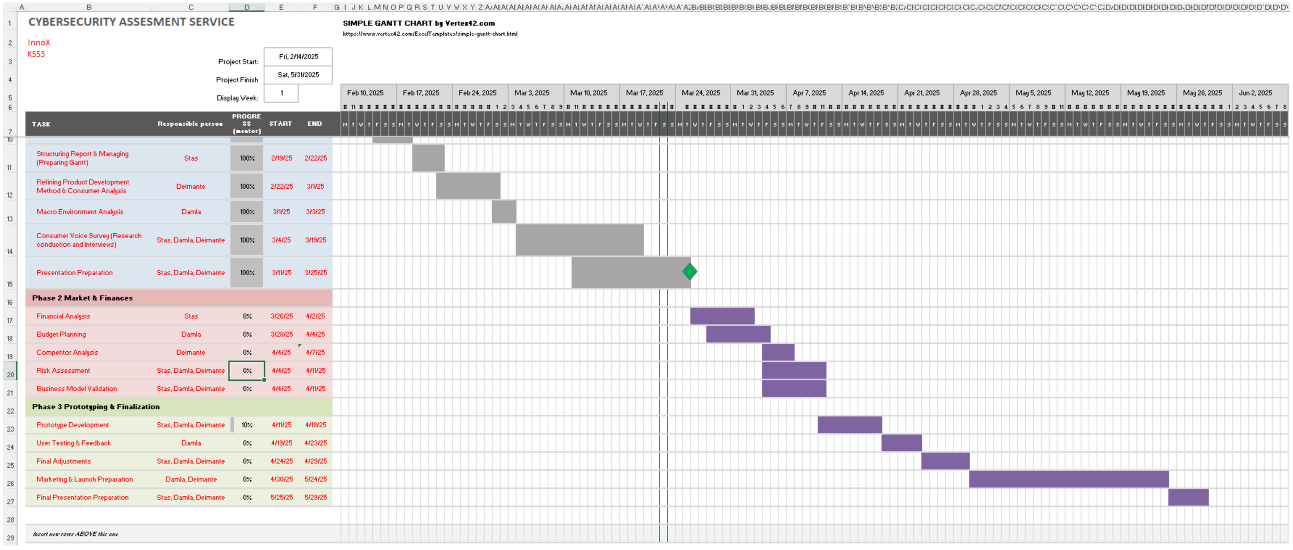
We started by talking to business representatives to hear firsthand about their challenges with cybersecurity. These coversations shaped our understanding of the issue and helped us define the core problem: eventhough there a lot of companies that do, there are still a lot that don’t have the tools or training to properly evaluate and respond to cyber threats.

Next, we brainstormed different solutions and decided to focus on a service that combines simulated cyberattacs with clear, actionable reports and employee training. To keep everything organised, we built a Gantt chart (see Fig. 2) to map out the project timeline, key tasks and deadlines. Each team member took a roles based on their strengths:

- **Stanislav** worked on project planning and technical research
- **Damla** handled the competitive landscape and interview process
- **Deimantė** focused on market insights, report writing and shaping the overall direction

We used WhatsApp and regular in-person meetups to communicate, share updates and keep everything moving smoothly.

Overall, this method has helped us stay focused, adapt quickly, and create a service that's grounded in real-world needs.



CYBERSECURITY ASSESMENT SERVICE

InnoX
K553

Project Start: Fri, 2/14/2025
Project Finish Sat, 5/31/2025
Display Week: 1

SIMPLE GANTT CHART by Vertex42.com
https://www.vertex42.com/ExcelTemplates/simple-gantt-chart.html

TASK	Responsible person	PROGRESS (mentor)	START	END
Structuring Report & Managing (Preparing Gantt)	Stas	100%	2/19/25	2/22/25
Refining Product Development Method & Consumer Analysis	Deimante	100%	2/22/25	3/1/25
Macro Environment Analysis	Damla	100%	3/1/25	3/3/25
Consumer Voice Survey (Research conduction and Interviews)	Stas, Damla, Deimante	100%	3/4/25	3/19/25
Presentation Preparation	Stas, Damla, Deimante	100%	3/11/25	3/25/25
Phase 2 Market & Finances				
Financial Analysis	Stas	0%	3/26/25	4/2/25
Budget Planning	Damla	0%	3/28/25	4/4/25
Competitor Analysis	Deimante	0%	4/4/25	4/7/25
Risk Assessment	Stas, Damla, Deimante	0%	4/4/25	4/11/25
Business Model Validation	Stas, Damla, Deimante	0%	4/4/25	4/11/25
Phase 3 Prototyping & Finalization				
Prototype Development	Stas, Damla, Deimante	10%	4/11/25	4/18/25
User Testing & Feedback	Damla	0%	4/19/25	4/23/25
Final Adjustments	Stas, Damla, Deimante	0%	4/24/25	4/29/25
Marketing & Launch Preparation	Damla, Deimante	0%	4/30/25	5/24/25
Final Presentation Preparation	Stas, Damla, Deimante	0%	5/25/25	5/29/25

Insert new rows ABOVE this one

Fig. 3. Gantt Chart of Cybersecurity Assessment Service Project

2. Product Development Concept

The concept of product development requires critical examination of different factors affecting the cybersecurity assessment service. This section of the report examines the macroenvironmental part, customers' opinion, and competition.

2.1 Macro Environmental Analysis

Macro environmental analysis of the cybersecurity market identifies significant forces that influence the demand and expansion of our service. They include technological, economic, legal, sociocultural, and environmental forces.

Technological Factors: Increased complexity of cyber systems and emergence of remote work environments have raised greater opportunities for cyber attacks. Phishing's fast-evolving nature requires more adaptive and real time cyber security solutions. Cybersecurity Ventures (2022) predicts global cybercrime spending to reach $10.5 trillion by 2025 (Cybercrime To Cost The World $10.5 Trillion Annually By 2025), up from $3 trillion in 2015. This reflects the scale of loss and requirement for a good cyber security.

Economic Factors: Rising costs of cyber attacks impose significant burdens on companies. IBM's Cost of a Data Breach Report (2024) states that the average cost of a data breach rose to $4.45 . Macro environmental analysis of the cybersecurity market identifies significant forces that influence the demand and expansion of our service. They also include technological, economic, legal, sociocultural, and environmental forces.

Technological Factors: Increased complexity of cyber systems and emergence of remote work environments have raised greater opportunities for cyber attacks. Phishing's fastly evolving nature requires more adaptive and real time cyber security solutions. Cybersecurity Ventures (2022) predicts global cybercrime spending to reach $10.5 trillion by 2025 (Cybercrime To Cost The World $10.5 Trillion Annually By 2025), up from $3 trillion in 2015. This shows the scale of loss and requirement for efficient cyber security solutions.

Economic Factors: Rising costs of cyber attacks impose significant problems on companies. IBM's Cost of a Data Breach Report (2024) states that the average cost of a data breach to $4.45 million in 2023, a 15% rise compared to the last three years (Cost of a Data Breach Report 2024). With cybersecurity spending expected to reach $188 billion globally by 2025, economic factors become the priority in motivating companies to invest more in prevention services.

Legal Factors: Compliance shows like the General Data Protection Regulation (GDPR) in the European Union and the U.S. Cyber Incident reports for critical Infrastructure Act (CIRCIA) have increased the importance of compliance. Failure can lead to heavy financial penalties. GDPR, for example, has already collected over €4 billion in fine since 2018 (GDPR Enforcement Tracker Report).

Sociocultural Factors: Human mistakes are still the main reason for cybersecurity incidents. Verizon's 2023 Data Breach Investigations Report highlights that 74% of breaches have the human aspect (Data Breach Investigations Report). Organizations are increasingly emphasizing training and awareness programs to address risk, demand for cybersecurity services that tackle behavioral change.

Environmental Factors: As less apparent, the environmental impact of digital infrastructure is growing. It's estimated by the International Energy Agency (2023) that data centers alone use around

1% of general electricity usage (Data centres and data transmission networks). Sustainability concerns are gradually impacting digital service design, such as cybersecurity.

These are the factors that have a direct impact on designing and offering our cybersecurity testing service. Our service is designed to not only provide testing and simulation but to address compliance and awareness as well in line with regulatoryy and market requirements.

2.2 Consumer Voice Survey

To better understand user needs and validate our product concept, we conducted qualitative research with industry professionals. While a broader survey was originally planned, previous limited responses led us to adopt an interview based approach.

We carried out five semi structured interviews with practitioners from various backgrounds including estate, manufacturing, eccommerce, investment. Each interview lasted approximately 30–45 minutes and was conducted online. Interviews were transcribed and theme analyzed in order to identify recurring patterns and learnings.

Key findings:

- ImmoScout24: Mentioned the importance of internal coperation with external specialists and AI based phishing simulation. Stressed that employees won't be serious about cybersecurity until after a breach.
- Ditaş Doğan A.Ş.: Described an experience of a simple phishing attack because of employee fault. Called for available awareness training, especially for elderly employees.
- E commerce platform: Mentioned phishing and insider data breach. Suggested individualized training sessions and simulated phishing improved overall preparedness.
- Investment & EdTech company: Witnessed disparate levels of awareness among the staff and suggested regular communication on Slack and regular short trainings.
- Executive Coach & Psychologist: Used words to describe non tech savvy individuals who did not have easy use tools. Helped in promoting behaviorally based training.

Research Objectives:

a) Analyze cybersecurity awareness and preparedness among businesses by examining current security policies and past incidents.

b) Analyze how a business operates and how employees handle security to find weaknesses that hackers could exploit, such as falling for fake emails (phishing) or being tricked into sharing sensitive information.

c) Evaluate the perceived necessity and potential adoption of cybersecurity assessment services, including controlled attacks and training.

Interview questions:

General Information

1. Can you briefly introduce your company and your role within it?

2. What are your main responsibilities related to IT and cybersecurity?

Cybersecurity Threats & Past Incidents

3. Has your company experienced any cyberattacks or security breaches? If so, what was the impact?
4. How did your company respond to the incident? What worked well, and what could have been improved?
5. How concerned are you about cybersecurity threats affecting your business operations?

Employee Cybersecurity Awareness

6. On a scale of 1 to 10, how aware do you think your employees are of cybersecurity risks?
7. Does your company currently provide cybersecurity training for employees? If so, what does it include?

Interest in Our Service

8. Do you believe your company would benefit from a service that simulates cyberattacks and assesses vulnerabilities? Why or why not?
9. What would make such a service more valuable to you? (e.g., phishing tests, penetration testing, real-time threat analysis)
10. How often do you think businesses should conduct cybersecurity assessments?

Cybersecurity Training & Guidance Needs

11. What key topics do you think cybersecurity training should cover for employees?
12. Would you prefer cybersecurity training as interactive workshops, online courses, or periodic awareness sessions?
13. What challenges do you face in ensuring employees follow cybersecurity best practices?

Results summary:

An interview with one of the representatives of ImmoScout24, a leading real estate service provider in Germany, Austria, and Spain, was provided valuable insights about the company's cybersecurity practices. According to the representative, large companies like ImmoScout24 typically have independent cybersecurity departments that take care of activities such as simulated phishing attacks and conducting multiple employee awareness workshops each month. But they stated that this activity can be built upon further, especially in response to technological changes. For example, new devices can replicate the voice of a company's CEO or even produce videos with the CEO, something that could be utilized to attack internal cybersecurity teams and raise awareness.

Additionally, the interviewee, being based in the data science unit, said his top priority is internal cybersecurity as compared to guarding against external penetration attempts. He said his team has not fully investigated newer types of social engineering yet, and therefore, it's necessary to gain a better grasp and training in the same so that their overall cybersecurity position gets stronger.

An interview to gather opinions on cybersecurity with the IT Manager of Ditaş Doğan A. Ş., a company that specialised in automobile parts. Said that two years ago, an employee unintentionally downloded a file that encrypted data, resulting in a cyberattack on theır company. The breach caused disruption even thougth the organization had backups in place, which led them to apply stricter security procedures.

Also, they pointed out that despıte higher management being more knowledgeable about cybersecurity these days, budget constraints are still a threat and some decision makers still consder cybersecurity as a value added. In response to a question about employee awareness, they noted that

many workers, particularly those in older age groups, are unaware of cybersecurity risks, regularlly take risks by using weak passwords and clicking on dubious links.
They also said how important it is to give staff members hands on, interactive training on subjects like phishing awreness, password security, and dangerous links.

Interviewed with the CISO of a Turkish ecommerce platform about information security that is being used by the company. An employee leak login data combined with a phishing event last year, the organization received many ddos and phishing attempts. While there are still workers who mistakenly believe cybersecurity is a relatively smal technical issue, the CISO said, more senior ranks do now view it as a threat to the business. Phishing and cybersecurity is understood by employe; IT teams were the serious ones, while sales and customer support didn’t know much.

The CISO strongly recommended what basically amounts to vulnerability assessments and cyberattack simulation services, noting that they are able to see cracks and vulnerabilities ahead of time before hackers and to give staff members hands on training. Cybersecurity training for employees should cover topics such as phishing awareness, password security knowledge, safe internet browsing, and identifying suspicious activity. You get more out of insttruction when it is applied during simulated attacks rather than theoretical knowledge.

Another interview was conducted with a member of the board Education Technology and Inventor Capital Group, who is deepley engaged in technology and investment secotr. The interviewee indicated that one of their portfolio companies is working closely with the cybersecurity assosciation of Lihuania to develop cybersecurity solutions and offer training to companies. Therefore, cybersecurity is a familiar and serious problem in their company.

The inventor said that though the employees do undersand something about cybersecurity, the degrees vary, and regular training is the solution. The team uses social reminders like jokes trough Slack in an effort to maintain good practises. The firm also intends to obtain ISO certification and thereby best practise in cybersecurity. One of the potfolio companies is in the military-related industry, hence posing a higher threat of targeted cyber attacs. Even though they did not experience direct attacks, theinterviewee recalled a previous instance of data loss due to an error by one of the developers – a cautionary tale about threats from within.

They supported the idea and recommended including adherence cybersecurity standards. They also suggested examining CyberUpgrade a new Lithuanian company engaged in cybersecurity with a great market potential.

The last interview was conducted with an executive coach and psychologisy lecturer who also runs an Instagram account focused on digital awareness and online behaviour. She advises managers and businesses, walking them trough issues they encounter with digital behaviour, namely on social media. As far as cybersecurity is conserned, she emphasized its importance not only to businesses but also to individuals. While she herself has not experienced a cyberattack, she gets suspicious emails very frequently and is sure of reconizing them because of her ongoing interest in the topic and regular reading.

When asked about the proposed cybersecurity audit service, she replied that she was very much in favor of the idea. She said awareness levels are very varied among individuals and businesses, and having an easy-to-understand, straightforward guide in Lithuania would be of great value. While she currently has some safety measures in place and does not feel an urget need for additional services, she appreciated the idea of such a service being an option when it is needed – especially for those with less technical knowledge, such as earlier generations.

Conclusions:

The interviews highlighted that phishing attacks remain a significant risk, with employee errors leading to security breaches. While management awareness is increasing, budget limitations and insufficient training persist, especially among non-IT staff. Hands-on training and vulnerability assessments were recommended to improve cybersecurity. We saw that the simulated phishing should be constantly upgrading and there could be a lot of different way of how we can emplement it, such as using an AI generated video. The big companies could already have a cyber security department, but there work still could be enhaced.

2.3 Consumer Analysis

Our target clients are organizations and businesses that value cybersecurity but lack the in-house resource to properly assess and improve their security position. Based on our market research, we have identified several key consumer segments that stand to benefit most from our service.

1. **Small and Medium enterprise:**

   These companies are likely to have limited IT staff and budgets and might not have the ability to pay for security reviews on a regular basis. They are more vulnerable to unpatched systems, social engendering and phishing. Our service provides a cheap and easy method for the, to become aware of their vulnerabilities and train personnel without having to maintain large internal personnel.

2. **Large Corporations:**

   Although large businesses usually maintain specialized cybersecurity teams, they too can be aided by external reviews and worker training. Our customized simulations and reports provide an outside viewpoint and assist in confirming the adequacy of current measures. Moreover, large businesses usually must prove compliance with industry guidelines, which our service facilitates.

3. **Educational Institutions:**

   Universities and colleges contain a great deal of personal and sensitive data – from student records to research information. They have little resources devoted to cybersecurity in most cases. Our service helps these institutions identify vulnerabilities and educate staff and students about safe online habits.

4. **Government and Public Sector Organizations:**

   Government agencies handle sensitive and frequently classified information. Small security breaches can have disastrous consequences. Our service provides a proactive way of identifying and minimizing risks trough-controlled testing and awareness campaigns, which is particularly vital in the public sector.

5. **IT and Tech Companies:**

Ironically, even tech firms can get it wrong inside. From high-speed development cycles or complacency regarding technical staff, loopholes can sneak in. Our service offers a vital doble-check layer – especially directed at human factors like employee sensitivity and response.

In each of these consumer groups, one common issue exists: an imbalance between technical protection and human cognition. Most leaks do not happen due to advanced attacks, but due to usual mistakes – clicking an embedded link or sharing confidential information with someone pretending to be friendly. That's where our combination of testing and training prevails.

By focusing on these core consumer segments, we're ensuring our solution is relevant and valuable to a wide range of organizations aiming to strengthen their cybersecurity from the inside out.

After evaluating all segments, SMEs are the most attractive and strategic target for out business. This is due to:

- High vulnerability and low internal cybersecurity maturity
- Growing pressure to comply with EU cybersecurity frameworks
- The opportunity to build long-term relationships as their tech stack grows

By addressing this segment, we tap into a wide customer base with urgent needs and limited alternatives.

2.4 Analysis of Competitors

The cybersecurity sector in Lithuania and Europe is growing rapidly, with many providers offering protection tools, consulation and complience support. To position our service effectively, we conducted a competitor analysis focusing on direct and indirect players in the cybersecurity assesment space.

- Direct competitors: Firms offering simulation-based assessments, training or potential testing (NRD Cyber Security, Cyber Update).
- Indirect competitors: General IT consultants or infrastructure-focused companies offering

These companies often emphasize infrastructure audits or governance policy, leaving a gap in human-factor-focused simulations, which is where our solution thrives.

We have contrasted a variety of big players in Lithuania and Europe offering cybersecurity services similar to ours. Below is the table outlining their strengths and weaknesses.

Table **2**. Competitors' weaknesses/strengths.

	Secmentis	**NRD Cyber Security**	**Cyber Upgrade**
Strengths	-Comprehensive Service portfolio -Global reach -Strong focus on proactive defence strategies.	-Specialization in cybersecurity strategy, policy and infrastructure -Strong presence in the Baltic region -Public sector partnerships.	-Offers continuous vulnerability scanning and employee training -Emphasis on AI-driven monitoring

Weaknesses	-.Limited public info about internal structure and team -Low brand visibility outside niche.	-Focuses more on consulting/governance than hands-on testing -May be seen as complex for smaller clients.	-Less known in the broader EU market. -Services may lack full customization for different sectors.

We can observe trough this analysis that even though these organizations do good business, most of them heavily focus on either infrastructure or strategy with less focus on the human aspect of cybersecurity, i.e., employee behavior and response awareness in real time.

This gives our project a great competitive edge – by margin simulated attacks with customized reporting and in-person employee training, we don't simply inform individuals where systems are vulnerable, but also why they're vulnerable and how to not become vulnerable trough a change in behavior.

Our goal is to be an interface between technical analysis and everyday digital know-how, especially for schools, universities and companies that lack professional cybersecurity personnel.

2.5 Supplier Analysis

In order to have our cybersecurity analysis service successfully operational, we depend on several key categories of providers and external products that complement the technical as well as operations aspects of the service, Our providers are crucial for keeping our product quality, secure, as well as scalable.

Major supplier classes:

Suppliers of cybersecurity software: we employ phishing simulators such as GoPhish, vulnerability scanners such as Nessus or OpenVAS and penetration testing software such as Metasploit. All of these are necessary to simulate real attacks and identify variabilities.

Cloud infrastructure services: hosting, storage and data encryption are handled by cloud providers such as AWS, Microsoft Azure or EU-based Hetzner, chosen due to thei compliance with GDPR and having high-security standards.

Training Platforms: to offer structured cyber awareness training, we plan to use software like TalentLMS, allowing us to track employee progress and customize learning pathways.

UI/UX and report design tools: software like Figma and Canva allow us to create a user-friendly web interface and visually separate reports, displaying intricate data in a more consumable format to clients.

Legal and Compliance Consultants: we can engage legal experts in GDPR legislation to ensure that everything we do in simulation, data processing and reporting is legal and ethical.

Trough alliances with vetted and competent suppliers in every one of these areas, we ensure our service is sound technically in accordance with the law and intuitive.

Chapter 2 gave us a comprehensive view of the environment our product will operate in. Trough macro analysis, consumer research, competitor evaluation and supplier review, we’ve identified a clear opportunity in the market. There is a growing need for cybersecurity services that not only test systems but also focus on human error often the weakest link. By combining technical testing, visual reporting and personnel-focused training our service meets that requirement in a way that is both understandable and scalable. The results herein will guide further iteration and development.

2.6. Financial Analysis

The aim - to calculate income, expenses and expected profits based on market, competitor, and consumer data analysis, and to define the funding sources.

Questions for financial prognoses:

1. What costs are required for product development, prototyping, testing?
2. What income and costs are forecasted for the first year of activities?
3. What are the expected start-up sources of financing?

2.6.1. Costs for product development, prototyping and testing

Our team consists of three people, thus for prototyping phase we used our own devices (computers, phones and one tablet), contributed our personal time by attending regular meeting, ideating, discussing and shaping our start-up. We did not pay for any services and development of our product, since we used the open-source product as a basis. No outside software development expenses were incurred because the product was developed using the open-source GoPhish platform. The anticipated development costs are broken down below in Table 1. according to the time, transportation, and equipment consumption values.

We computed the device expenses based on an average cost of €1,000 per unit, amortized over a 12-month period, and accounted for 4 months of utilization during the project. We assessed the average remuneration for junior managers at €1,500 per month (which is around €10 per hour) to account for the value of the team's time dedicated to management and concept creation. As we had 2 seminars 1.5 hour each a week and 4 weeks for this task 24 hours including our own time besides seminars.

Table 3. The product development costs

Type of costs	**Value, eur**
Use of 3 computers *(3 × €1,000 / 12) × 4*	€1,000
Use of 3 phones *(3 × €1,000 / 12) × 4*	€1,000
Use of one tablet (*€1,000 / 12) × 4*	€350
Team time for idea generation & implementation *24 × 3× 10€*	€720
Transportation (car and gas for meetings)	€500
Total costs:	€3,570

The total cost of development of the prototype is €3570. Although no direct cash outlays were incurred for software or services, this amount represents the value of resources utilized by the team, encompassing equipment, time, and travel.

2.6.2. Income and costs for the first year of activities

Questions for income and costs forecast:

- What assets (long-term) are needed for the operation?
- What is the forecasted income from the sale of the product? What resources are needed to carry out a product and activity? What are the forecasted costs of the product?
- What is the forecasted result of the activity - profit (loss)?

Initial investments into long-term assets

In order to properly establish our business and make long term growth, we will invest in crucial long term assets that benefit both our functioning and technical abilities. First, we will purchase computers for all 11 employees at a cost of about €1,000 each, which will amount to €11,000. We will also invest €6,000 in office installation, such as furniture, desks, chairs, and other basic infrastructure to be able to work in a prooper setting. To finance internal operations and cybersecurity measures, we will invest €7,000 in servers, networking devices, and other computer equipment.

Since cybersecurity demands continuous simulation and testing, we will set up a tiny test lab internally at a cost of €4,000 comprised of different devices as well as software environments. To ensure that we work securely from the start, we will invest €3,000 in long erm license expenditures on cybersecurity equipment such as firewalls, VPNs, as well as antivirus software.

For online visibility and client interaction, we will invest €5,000 to create and design our website and client dashboard platforms. We will also purchase €2,000 worth of video and training equipment to produce educational and marketing content. For branding assistance, €1500 will be invested in visual design and branding materials.

In addition, €500 will be spent on technical books and professional materials to aid our team's growth, and €3,000 will be spent on project management and CRM software licenses to automate internal processes and client relationships.

Overall, our overall investment in long-term assets will be around €43,000.

Table 4. Initial investments into long-term assets

Type of long-term asset	Value, eur
Server & Network Hardware	€7,000
Computers (11*1000)	€11000 =€1000*11
Office Setup (tables, general office setup)	€6000
Security Software Licenses (1-year+)	€3,000
Internal Test Lab Setup (for simulations)	€4,000
Video/Training Equipment	€2,000
Brand Design Assets	€1,500
Technical Books & Reference Materials	€500
Initial Software Tools (Project Mgmt, CRM)	€3,000

Total	€43,000

Income forecast

Based on the market, competitor, and consumer need analysis, we have developed a pricing strategy for our cybersecurity service packages. We will offer 3 month service packages from €1,000 to €10,000 depending on the client size and services needed. These packages will include:

- Simulated phishing and cyberattack tests
- Detailed security assessment reports
- Cubersecurity training sessions

We anticipate having two significant types of clients:

• SMEs (Small and Medium Enterprises) would typically purchase packages ranging from €1,000–€5,000.

• MNCs (Multinational Corporations) would typically require high end, customized services ranging from €5,000–€10,000.

Table 5. Income forecast

Quarter	Clients	Revenue
Q1	2 SME - 3 MNC	€22,000 - €50,000 (full service covering simulated attacks, reports, and training)
Q2	5 SMIE - 5 MNC	€55,000 - €100,000
Q3	7 SMIE - 8 MNC	€87,000 - €150,000
Q4	9 SMIE - 11 MNC	€119,000 - €200,000
Total	**50**	**€283,000 – €500,000= €783,000**

Expenses forecast

The subsequent expense estimate determines the anticipated starting and operation costs of the Cybersecurity Assessment Service for its inaugural year. Based on supplier research, technical spec, and approximate resource needs, this estimate gives quarterly details of significant cost categories such as materials, marketing, operating expenses and technological stuff. The prediction seeks to present a realistic picture of the funds neded to establish, sustain, and market the service in a way that makes it sustainable and scalable from the beginning.i

Table 6. Expenses forecast

Category	Q1	Q2	Q3	Q4	Total
Materials & Software Licenses	400	300	300	300	1,300
Marketing & Promotion	600	400	400	400	1,800
Operating Costs (utilities, internet, etc.)	300	300	300	300	1,200
Cloud Hosting / Servers	150	150	150	150	600
Equipment Depreciation	200	200	200	200	800
Domain, Tools & Subscriptions	100	100	100	100	400
Legal & Admin Costs	250	0	0	0	250
Research & Development	500	400	300	200	1,400
Miscellaneous	100	100	100	100	400
Total	**2,600**	**1,950**	**1,850**	**1,750**	**8,150**

2.6.3. Forecast of payroll costs

To reflect the job market, we updated average net and gross salaries using realistic assumptions. Based on typical local salary data, we used net monthly salaries and applied a gross-up multiplier of approximately 1.68. This estimation accounts for employer taxes and social insurances contributions and reflects average total workplace costs.

We forecasted salaries for 11 employees across key functions: management, cybersecurity, development and marketing.

Table 7. Payroll costs (employees directly involved in the production of the product/ provision of the service, sales, administration, management staff)

Position/ Profession	Number of employees	Average wage after taxes (net wage), eur per	Total workplace costs[1], eur	Quarterly wage fund, eur

		employee per month		
Manager	2	1815.00	3053.10 * 2 = 6,106.2	3 x 6106.20 = 18,318.60
Senior Cybersecurity Specialist	2	1815.00	3053.10 * 2 = 6,106.2	3 x 6106.20 = 18,318.60
Senior Web developer	2	1815.00	3053.10 * 2 = 6,106.2	3 x 6106.20 = 18,318.60
Cybersecurity Specialist	2	1510.00	2516.33* 2 = 5032.66	3 x 5032.66 = 15,097.98
Web developer	2	1510.00	2516.33* 2 = 5032.66	3 x 5032.66 = 15,097.98
Marketing Specialist	1	1400.00	2306.14*1 = 2306.14	3 x 2306.14 = 6,918.42
Total:	11			92,070.18

The payroll costs presented in Table 6 are based on typical salaries found in Lithuania's ICT and cybersecurity sectors, especially in Kaunas. The net monthly wages were selected by reviewing publicly available job listings, national statistics, and industry benchmarks relevant to roles such as cybersecurity specialists, developers and digital marketing professionals.

To estimate the total employer cost, we applied a gross-up multiplier of approximately 1.68. This figure reflects standard employer contributions in Lithuania, which include:

- Social contributions to "Sodra"
- Health insurance payments
- Guarantee and long-term employment fund contributions
- Applicable payroll taxes

The multiplier ensures we capture the full cost to the employer, not just the employee's take-home pay. These calculations are commonly used in Lithuanian financial planning when estimating organizational payroll expenses.

In this table:

- The monthly total workplace cost per role is calculated by multiplying the net salary by the approximate gross-up rate.
- The quarterly wage fund reflects three months of costs for all employees in each role.

Based on this model, the total quarterly wage fund is 92,070.18 euros, resulting in an annual payroll cost of approximately 368,280.72 euros. This budget supports a team of 11 employees across management, cybersecurity, development and marketing functions, providing a solid human capital foundation for the operation of the cybersecurity assessment service.

Calculation of depreciation

We applied the straight-line depreciation method to allocate the cost of long-term assets over their estimated useful life. This method assumes that assets lose value eventually over time, which is standard for early-stage financial planning.

The table below reflects the long-term assets we plan to use – form computers and servers to branding and cybersecurity software. We excluded short-lived or non-depreciated items such as technical booked and our website platform, since they either don't lose significant value over time or are considered one-off costs.

Table 8. Depreciation of long-term assets

Long-term assets	**Cost of asset, eur**	**Residual value, eur**	**Estimated useful life, years**[1]	**Quarterly charge for depreciation, eur**[2]
Office Equipment	6,000	1,000	8-10	125,00-156,25
Computers (11 units)	11,000	2,200	5	440,00
Internal test lab setup	4,000	1,000	4	187,50
Servers & network devices	7,000	1,400	5	280,00
Security Software Licenses (1 year)	3,000	0	1	750,00 (1 year amortization)
Video & Training equipment	2,000	400	3	133,33
Branding Design Assets	1,500	0	3	125,00
CRM & Project management tools	3,000	0	1	750,00
Total:	37,500			~2,790.83 per quarter

Each item in the table represents a real tool or resource we need to deliver quality cybersecurity services. For example, our internal test lab setup – which includes devices and simulation environments – is essential for running controlled cyberattacks. The Sofware licenses and CRM tools will help us manage client data and daily operations securely and efficiently.

- Larger assets, like office furniture and servers, are spread over longer periods (4-10 years).
- Shorter-lived items, such as licenses or project management tools, are depreciated faster – usually within one year.

On average, we estimated that around 2,805 euros of deprecation will be recorded per quarter. While deprecation isn't a "real" cash expense, it is important for showing how asset value changes over time and ensuring our financial planning reflects the lifecycle of our tools and equipment.

Forecast of operating expenses (overheads)

To run our cybersecurity service effectively and maintain day-to-day operations, we forecast a range of operating expenses that recur either monthly or quarterly. These are essential for keeping the business functional and visible in the market.

Our overhead costs are broken down as follows:

- Rent and cleaning services – estimated at 5,000 euros per quarter for an office space suitable for an 11 person team in Kaunas.
- Advertising and branding – budget at 12,500 euros per quarter to build awareness, attract clients and promote our services both online and offline.
- Accounting services – projected at 1,500 euros to 6,000 euros per quarter, with some additional administrative costs in Q4 due to year-end reporting and external consultation.
- Communications and utilities – including the internet, electricity, phone and cloud-based communication tools, budged at 1200 euros per quarter.
- Start-up costs – a one-time amount of 1000 euros incurred in Q1 for business registration, legal setup and initial software configurations.

These values are summarized in table 8 under the “Operating expenses” category. The total forecast overhead expenses for the first year amount to 86. , with slight variations per quarter based on business needs.

This budget ensures we maintain operational stability, reach potential clients, and provide a professional working environment for the team without overspending.

Estimated profit and profitability

To provide high-quality cybersecurity services and ensure smooth business operations, we plan to employ a team of 11 professionals across key roles such as management, cybersecurity, development and marketing. The payroll structure reflects average net wages in the region for each position. The detailed quarterly payroll expenses are summarized in Table 6. The total projected payroll cost for the first year is €92,070.18.

We plan to invest approximately €43,000 into long-term assets, including computers, office setup, networking hardware, and software tools. These assets will be gradually depreciated over their useful life in accordance with standard accounting practices.

According to our calculations, these assets generate a quarterly depreciation charge of approximately 2,805 euros, as shown in table 7. This allows us to track the declining value of these tools over time ein a realistic way, without affecting short-term cash flow.

Despite the expected setup loss in Q1 and continued investments in Q2, the business is forecasted to become profitable in Q3 and generate significant earnings by Q4. This reflects the scalability and demand for cybersecurity services in the Lithuanian market.

Table 9. Estimated profit and profitability

Estimated profit and profitability

	I qtr, eur	**II qtr, eur**	**III qtr, eur**	**IV qtr, eur**	**Total, eur**
Income	**50,000**	**100,000**	**150,000**	**200,000**	**500,000**
Expenses, total	**112,570**	**113,070**	**113,070**	**116,070**	**454,780**

Payroll	92,070	92,070	92,070	92,070	368,280
Operating expenses, total	20,500	21,000	21,000	24,000	86,500
Rent, cleaning	*5,000*	*5,000*	*5,000*	*5,000*	*20,000*
Advertising	*12,500*	*12,500*	*12,500*	*12,500*	*50,000*
Accounting services	*1,500*	*3,000*	*3,000*	*6,000*	*13,500*
Communication, utilities	*1200*	*1200*	*1200*	*1200*	*4800*
Start-up costs[1]	*1000*	-	-	-	*1000*
Profit (loss) before interest, taxes, depreciation and amortization (EBITDA)	**-62,570**	**-13,070**	**36,929**	**83,929**	**45,219**
Depreciation	2,805	2,805	2,805	2,805	11,220
Financial expenses (interest)	0	0	0	0	0
Profit (loss) before taxes	**-65,375**	**-15,875**	**34,125**	**81,125**	**34,000**
Profit tax[1]	**0**	0	0	0	0
Net profit (loss)	-65,375	-15,875	34,125	81,125	34,000
Net Profit Margin, % $NPM = \frac{Net\ profit\ (loss)}{Income} * 100$	-130.75%	-15.88%	22.75%	40.56%	6.8%

By the end of the first year, we project a net pre-tax profit of approximately 34,000 euros. This result is strong for a new service-oriented startup, especially considering the upfront investments in marketing and infrastructure.

The structure of our costs reflects a healthy balance between growth spending and long-term sustainability. As client acquisition improves and fixed costs remain stable, we expect this profitability to increase steadily in subsequent years.

2.6.4. Sources of financing

To fund the substantial upfront cost, especially salaries and fixed assets, the project will seek a combination of funding sources. Fixed initial capital will be funded through a bank loan. Additionally, the team aims to offer a minority stake, well established cybersecurity or technology company for strategic support and funding. To keep minimum upfront costs on large equipment, we will be leasing long term assets such as laptops and servers. Finally, stock based crowdfunding will be employed to stimulate early stage followers and generate buzz and raise additional funds. The hybrid method minimizes financial risk but promotes flexibility in year one of operations.

Conclusions

The cyber security assessment service is financially viable in the long run, meeting a growing demand with no internal security capability. Even though the initial year has a predicted loss due to high wage and development costs, the service is in a good position for good revenue growth as the number of customers increases. With proper funding and cost control, our company can be profitable during the second year, especially with repeat business, expanded offerings, and reduced startup costs. The financial situation looks much better if some of the team costs are financed externally or deferred.

3. Product Development

Completeness:

- Decided project goals, objectives, and selected technology.
- Defined the roles and responsiblities of the team.
- Did interviews with potential users to make research.
- Conducted research which helped in analyzing user needs and wants.
- Evaluated macroenvironmental factors.
- Did supplier analysis to have our cybersecurity analysis service operational.
- Evaluated macroenvironmental factors such as digital transformation trends, increasing cyber threats and regulatory requirements.
- Performed a supplier and resource analysis, identifying potential partners and tools required to support service delivery.

Goals:

- Assess cost structure, economic viability and resources needed.
- Make findings about the market and strategy.
- Assessing risks, and develop strategies.
- Evaluating sustainability and scalability.

List of references

1. Cybersecurity Ventures. (2022). (Cybercrime To Cost The World $10.5 Trillion Annually By 2025) (https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/)
2. IBM. (2024). (Cost of a Data Breach Report 2024). (https://www.ibm.com/reports/data-breach)
3. CMS. (2024). (GDPR Enforcement Tracker Report). https://www.enforcementtracker.com/
4. Verizon. (2023). (Data Breach Investigations Report) https://www.verizon.com/business/resources/reports/dbir/CMS. (2024). *GDPR enforcement tracker*. (https://www.enforcementtracker.com/)

~~4.~~5. Verizon.(2023).*DataBreachInvestigationsReport2023.* (https://www.verizon.com/business/resources/reports/dbir/)

~~5.~~6. International Energy Agency. (2023). *Data centres and data transmission networks*. (https://www.iea.org/reports/data-centres-and-data-transmission-networks)

~~6.~~7. Sodra. (2024). *Social insurance contribution rates*. (https://www.sodra.lt)

~~7.~~8. Investuok Lietuvoje. (2023). *Employee costs and taxation in Lithuania*. (https://investlithuania.com)