CyberCare Kymi

Cyber Simulation Training Environment

Janine Klauenbösch

XAMK Kaakkois-Suomen ammattikorkeakoulu
KYMEN LAAKSON LIITTO
Euroopan unionin osarahoittama
CyberCare Kymi

Table of Content

Glossary of Terms & Acronyms

Acronym /	English Term	Finnish Term / Selite
FTE	Full-Time Equivalent	Henkilötyövuosi (HTV) / työpanos
KPI	Key Performance Indicator	Keskeinen suorituskykymittari
SME	Small and Medium-sized Enterprise	Pk-yritys
ICT	Information and Communication Technology	Tieto- ja viestintäteknologia
NIS2	EU Directive on Security of Network and Information Systems (2nd version)	EU:n verkko- ja tietojärjestelmien turvallisuusdirektiivi (NIS2)
SOC	Security Operations Center	Turvavalvomo / tietoturvavalvomo
DoS / DDoS	(Distributed) Denial of Service	Palvelunestohyökkäys
EHR / EMR	Electronic Health / Medical Record	Sähköinen potilas- /terveystietojärjestelmä
ELY	Centre for Economic Development, Transport and the Environment	Elinkeino-, liikenne- ja ympäristökeskus
ESR+	European Social Fund Plus	Euroopan sosiaalirahasto +
ERDF / EAKR	European Regional Development Fund	Euroopan aluekehitysrahasto
H2020 / Horizon Europe	EU Research and Innovation Programme	Horisontti 2020 / Horisontti Eurooppa
HVA	Wellbeing county	Hyvinvointialue
SOTE	Social and Healthcare Sector	Sosiaali- ja terveydenhuolto
STM	Ministry of Social Affairs and Health	Sosiaali- ja terveysministeriö
THL	Finnish Institute for Health and Welfare	Terveyden ja hyvinvoinnin laitos

Executive Overview

This concept proposes a comprehensive cybersecurity training ecosystem for Finland's social and healthcare sector, combining three complementary tracks:

- Track A: VirtualLab Cyber Simulations (technical exercises)
- Track B: Table-Top Exercises (non-technical decision-making)
- Track C: Mini-Hospital Cyber Simulation (interdisciplinary, high-fidelity training)

The original intent was to anchor the programme in the Mini-Hospital environment. However, during development, the VirtualLab and Table-Top platforms emerged as scalable, cost-effective alternatives that offer high pedagogical value without requiring structural campus changes.

The Mini-Hospital track, while innovative, involves significant physical infrastructure investments—network cabling, simulation room integration, and specialised hardware. For long-term viability, it would require regular participation from 30–40 organisations annually, which is unlikely given the regional density of relevant companies. Without this volume, the investment may not be sustainable.

In contrast, the VirtualLab and Table-Top components can deliver effective training using laptops, portable kits, and remote facilitation. These tracks support scalable national deployment, require lower ongoing costs, and are more adaptable to evolving threats and regulation. However, for them to be fully functional, upfront investment is needed in platform reliability, scenario development, and facilitation capacity.

The full three-track model is technically feasible and pedagogically sound. However, for practical and financial reasons, it is recommended to prioritise development of the VirtualLab and Table-Top platform, with a future option to scale up to physical Mini-Hospital simulations where justified. This phased approach ensures early impact, long-term adaptability, and sustainable operations aligned with national preparedness goals.

Section 1: Concept and Value Proposition

Objective and Rationale

The concept aims to close a critical training gap in Finland's social and healthcare sector by offering accessible, scalable, and realistic cyber training to organisations of all sizes – from solo entrepreneurs to mid-sized businesses.

Why it matters

Cyber threats in this sector are growing rapidly, according to Enisas Threat Landscape (Abad et al. 2023, 3-4). Approximately half of all cyber incidents in this field are ransomware attacks. Yet, most providers – especially small and micro-businesses – lack the resources or options to train for cyber incidents. Existing alternative like the national cyber range of Finland in Jyväskylä (Jyvsectec) are often expensive, oversubscribed, and geared toward larger organisations.

Our Objective

To empower social and healthcare organisations with the capabilities and confidence to respond to cyber incidents by:

- Delivering affordable, browser-based exercises tailored to each organisation's size and capacity
- Enabling practical, scenario-based training that supports NIS2 compliance
- Leveraging existing platforms and partnerships to minimise costs and reduce duplication

Built on Proven Foundation

The solution builds upon two EU-funded projects – CyberCare Kymi and Kyberturvan tulevaisuus Kymenlaaksossa – which successfully piloted exercises with a wide variety of providers from different sectors, like social and healthcare. It also integrates the Mini-Hospital simulation environment, currently used in nursing education, by adding cyber disruption scenarios.

Together, this system allows flexible, modular rollout:

- Start with tabletop and virtual exercises for micro and small businesses
- Expand into live, interdisciplinary simulation when needed
- Support student training alongside professionals

This concept ensures that even the smallest social and healthcare providers in Finland have the tools and training to protect their patients, systems, and data – and positions the model for nationwide impact.

Target Audience & Sector Relevance

This training system is designed to be modular and tiered structured to ensure companies can engage in training appropriate to their size, operational complexity, and regulatory obligations. The trainings are for companies with 1-50 employees.

Social and Healthcare Providers

- Solo entrepreneurs
  Professionals such as therapists, nurses, and independent service providers often lack the resources for cybersecurity training, despite handling sensitive data. Tabletop and VirtualLab exercises provide low-cost,

accessible training opportunities without requiring advanced technical infrastructure.

- Micro and Small Companies (1-10 employees)
  Includes private medical practices, home care providers, and therapy clinics. These companies typically do not have in-house IT-personnel yet face real operational risk and potential legal obligations as big companies.
- Small-Medium to Medium Companies (11-50 employees)
  As digitalisation expands, these providers face more sophisticated cyber threats while still operating with limited budgets. They benefit from more advanced simulation-based exercises tailored to their scale and service model.

There are approximately 18 300 private social and healthcare companies in Finland, of which 95% are micro enterprises with fewer than 10 employees. (Rantakoski, 2023)

Government and Public Sector

- Wellbeing Service Counties
  These authorities are responsible for the organisation, funding, and delivery of social and healthcare services. Training participation supports operational continuity, inter-agency collaboration, and NIS2 compliance.
- National Agencies and Supervisory Bodies
  Involvement from oversight and policy-making entities ensures alignment with national strategies and facilitates standardisation of cyber preparedness across the country.

Under the NIS2 Directive, many organisations in the social and healthcare services sectors are classified as either “essential” or “important” entities. These are required to conduct risk assessments, implement incident response plans, and conduct regular staff training. (Directive (EU) 2022/2555, 85. article.)

Even organisations that are not directly subject to NIS2 may still face compliance requirements imposed by the wellbeing service counties. In 2024, updates to information management legislation introduced NIS2-based obligations for service providers. These include preparedness for denial-of-service attacks and, in some cases, regular cybersecurity audits mandated by the counties for their partner organisations. (Cybersecurity Act (NIS2))

Educational Institutions and Students

- Social and Healthcare Students
  Participation in exercises prepares students for real-world situations involving digital disruptions. Early exposure fosters readiness and supports sector-wide resilience. However, despite the increasing digitalisation of healthcare, cybersecurity and secure use of digital systems are still largely absent from formal social and healthcare training programmes. Many professionals begin their careers without having learned even the basics of information security, despite being expected to use digital systems responsibly and safely in client work. This gap in foundational training makes it significantly harder for them to adopt secure practices once in the workforce.
- Cybersecurity and ICT Students
  These students play a key role in designing, implementing, and facilitating both technical and process-oriented exercises. Their involvement builds technical and pedagogical capacity while providing hands-on experience that bridges the gap between theory and real-world application. Integrating student work in this way supports workforce development and long-term sustainability.

Technology Vendors and Service Providers

- IT Companies and Medical Device Providers
  These stakeholders gain insights by testing their solutions within realistic operating environments. This collaboration helps improve security, user experience, and technical resilience in real-world settings.

This inclusive targeting ensures the training ecosystem fosters a shared culture of cyber preparedness throughout the social and healthcare system – bridging public and private sectors, frontline professionals, management, students, and technology providers alike.

Key Features

This training environment combines technical, strategic, and immersive approaches into a modular framework tailored for Finland's social and healthcare sector, with an emphasis on accessibility, scalability, and real-world relevance.

Tree-Track Training Model

The concept is structured around three complementary tracks, allowing organisations to select the right level of training based on their size, technical maturity, and resource availability:

- Track A – VirtualLab: Technical cyber incident simulations delivered through a browser-based platform. Exercises are realistic, automated, and scalable – from solo entrepreneurs to mid-sized companies.
- Track B – Table-Top: Strategic, low-barrier table-top exercises that guide participants through decision-making and communication workflows using their existing response plan.

- Track C – Mini-Hospital: On-site, interdisciplinary simulations of live clinical and IT crisis in a controlled, hospital-like environment. Focused on mid-sized providers.

Each track supports specific roles (e.g. clinical, IT, leadership) and aligns with current regulations and laws.

Scenario -Based Learning

All exercises are grounded in real-world cyber incidents and escalate dynamically:

- Insider threats
- Phishing and ransomware
- Medical device failures
- Patient record system outages and data exfiltration
- Supply chain compromise
- DDoS

Each scenario includes branching paths, timed injects, and role-specific tasks, challenging participants to act under pressure and adapt their plans accordingly.

Role-Specific Participation

Exercises are designed to simulate realistic, cross-disciplinary cooperations:

- Clinical staff focuses on patient care continuity
- IT and cybersecurity personnel manage containment and recovery
- Leadership teams handle public communication and strategic coordination

This layered structure ensures that organisations can train as whole units, not isolated departments.

Integrated Feedback and Improvement

Post-exercise evaluation includes:

- Structured debriefings
- Performance feedback
- Improvement recommendations
- Playbook and response plan refinement

Tools are embedded into both the VirtualLab and the Table-Top platforms to support measurable progress.

Modular, Scalable Desing

- The concept is fully modular – Tracks A and B operate independently, allowing a phased rollout.
- Existing infrastructure and staff reduce setup costs (e.g. Mini-Hospital already used in nursing education; VirtualLab platform used in engineering education)
- Content reuse across tracks ensures cost-efficiency and faster scale-up
- Future-ready: structure allows expansion to other critical sectors beyond social and healthcare

Training Tiers and Simulation Catalogue (Tiers 1-3)

To support the broad diversity of social and healthcare providers in Finland, the training environment is structured in three tiers. Each tier aligns with the

organisation's size, complexity, and cybersecurity capacity, ensuring scalable value and appropriate training depth.

Tier 1 – Solo entrepreneurs and Micro Businesses

Target: Solo entrepreneurs and companies with 1-5 employees

Training Mode: Fully automated, remote-access simulations via VirtualLab and Table-Top

Key Features:

- Access to low-cost exercises on both platforms
- No technical setup required; browser-based delivery
- Non-technical scenarios, e.g.:
    - How can I continue caring for my clients, when my patient records are locked?
    - How do I inform clients and media in case of a breach?
- Built-in guidance and feedback
- Exercises available on-demand, 24/7
- Designed to support legal compliance and build baseline awareness

This tier ensures accessibility and removes technical and financial barriers for the smallest actors in the sector.

Tier 2 – Small Businesses

Target: Providers with 6-10 employees (e.g. small clinics, home care units)

Training Mode: Catalogue-based exercises with optional on-campus sessions

Key Features :

- Access to low-cost exercises on both platforms
- No technical setup required; browser-based delivery
- Scenario with non-technical table-top exercise and technical VirtualLab exercise
- Option for on-campus VirtualLab session with support
- Pre/post facilitation, structured feedback reports, debriefing
- Focus on multi-role training (management, clinical)
- Emphasis incident response improvement

This tier bridges the gap between non-technical and more advanced scenarios, building readiness for cyber incidents and team-based coordination.

Tier 3 – Medium Businesses

Target: Companies with 11-50 employees (e.g. medium-sized clinics and rehabilitation centres)

Training Mode: Hybrid Model (remote and on-campus)

Key Features:

- Full access to both platforms' catalogue
- Optional customisable VirtualLab and Table-Top exercises based on organisational structure
- Optional on-campus training (mini-hospital, VirtualLab)
- Pre-planning and post-exercise reports, debriefing
- Focus on cross-functional drills: leadership, IT, and care teams

This tier delivers higher-impact training to organisations with complex systems and regulatory responsibilities, while remaining affordable and flexible.

Exercise Catalogue Development Roadmap

Tier	Platform	Launch Scenarios (Y0-3)
1	VirtualLab + Table-Top	2-3 scenarios : each non-technical and simple technical
2	VirtualLab + Table-Top	2-3 scenarios: each non-technical and operational/technical
3	All platforms	2 scenarios: non-technical and advanced technical, + optional mini-hospital scenario

Benefits and Expected Impact

This multi-track training environment – anchored by the VirtualLab Cyber Simulation and the Table-Top Platform, and optional Mini-Hospital Simulation – delivers measurable impact on cybersecurity readiness, workforce skills, and sector-wide resilience. It provides inclusive, tiered access to realistic training while aligning with national legislation and long-term sustainability goals.

Improves Cyber Resilience Across the Social and Healthcare Sector

- Realistic, safe training environments prepare staff for digital crisis.
- Organisations can test and improve continuity plans and communications, and incident responses under simulated stress.
- Exercises are aligned with current regulations and laws, offering proof of compliance.
- Structured debriefings and feedback loops enable continuous improvement and iterative learning.

Measurable Outcomes: Key-Performance-Indicators

The environment is designed to deliver clear and trackable results, including:

Organisations trained / year

- Year 1: ~50
- Year 2: ~180
- Year 3: ~540
- Long-term scalability to thousands of annual users.

Exercises developed / year

- Baseline of 4 shared-use exercises (VirtualLab and Table-Top) by project start
- Annual addition of 4-6 new exercises, including sector-specific and customisable options

Demonstrated improvement in incident response

- Participants complete pre-/post-evaluation and feedback scoring
- Organisations gain actionable reports tied to cybersecurity readiness and risk management frameworks

Makes Cyber Training Affordable and Accessible

- Pricing scaled by organisations size: solo entrepreneurs pay as little as 80€ for a bundle of 2 exercises.
- No technical setup required for table-top and VirtualLab exercises.
- Remote access ensures participation from anywhere in Finland, regardless of geography.
- SMEs gain access to previously unavailable training options – closing a major national gab in cybersecurity capacity.

Enhances Interdisciplinary Skills and Workforce Capacity

- Role-based training for IT, clinical, management, and administrative staff improves cross-functional communication during crisis.

- Students from nursing, cybersecurity, logistics, and other IT fields participate in scenario designs, facilitation, and testing.
- Supports national workforce development and retention by embedding career-relevant learning in education.

Enables National Replication and Sectoral Expansion

- Modular design allows for replication beyond the Kymenlaakso region, helping other regions boost social and healthcare resilience.
- Dual-use scenarios and shared infrastructure models reduce development costs over time.
- Easily expandable to include other critical infrastructure sectors (e.g. energy, logistics, education, food supply).

Support Finland's Digital and Strategic Priorities

- Aligns with Finnish law and EU-wide initiatives on digital resilience and public service continuity.
- Fosters public-private cooperation: exercises bring together providers, vendors, regulators, and educators.
- Contributes directly to the national NIS2 implementation goals by offering a concrete training solution.

This environment empowers even the smallest organisations to meet their cybersecurity obligations – while offering advanced, scalable tools for more mature actors. Through its modular structure, national relevance, and measurable outputs, it presents a practical, sustainable response to Finland's growing cybersecurity training needs in this sector.

Section 2: Implementation Operations

This section outlines the practical steps required to move from concept to national service delivery. It includes the phased rollout plan, scenario development timelines, infrastructure setup, staffing, pilot testing, and evaluation criteria. The approach prioritises early delivery of low-barrier training for small providers, while building toward more complex, high-fidelity simulations in the Mini-Hospital environment.

Implementation Strategy

The implementation follows a phased approach to balance fast early impact with long-term capability building.

Tracks A and B can launch within the first project year, delivering immediate benefits for solo, micro and small companies. Track C is a multi-year, multi-project development requiring staged investment, procurement, and integration.

Guiding principles

- Early winds: Launch low-barrier, high-demand exercises quickly via browser-based platforms.
- Scalable growth: Add content, features, and tiers incrementally, avoiding downtime.
- Shared assets: Scenarios are developed to be used in bots Table-Top and VirtualLab as basis to reduce cost and speed-up delivery.
- Integration with education: Student projects and internships contribute to scenario creation, testing and facilitation.

Phase 1 – Preparation and Core Development (Months 0-6)

- Finalise requirements for VirtualLab and Table-Top Platform upgrades like user access, feedback, reporting, payment methods.
- Develop first four shared exercises (2 for solo/micro and 2 for small companies).
- Begin Mini-Hospital system requirements and infrastructure planning.
- Produce outreach materials and pricing models for Tier 1 and 2.
- Begin customer onboarding, training calendar, and early marketing.

Outcome: Ready-to-Launch core services for browser-based training, foundation laid for physical simulation.

Phase 2 – Initial Rollout (Months 6-12)

- Launch VirtualLab and Table-Top Platform to external clients
- Continue exercise development for Tier 1 and 2.
- Start Mini-Hospital procurement proves (hardware, software, integration services).
- Continue Marketing.

Outcome: Nationally accessible cyber training for small providers; Mini-Hospital moves into build phase.

Phase 3 – Service Expansion (Months 12-24)

- Expand Track A and B catalogue with role-based and sector-specific exercises.
- Offer on-campus simulations for medium providers.
- Install and configure Mini-Hospital infrastructure.
- Develop Mini-Hospital exercise.

- Introduce analytics dashboard and automated evaluation tools.

Outcome: Growing customer base; physical simulation infrastructure nearing completion, mini-hospital exercise planned.

Phase 4 – Refinement and Mini-Hospital exercise completion

- Collect technical, pedagogical, and participant feedback for Track A and B
- Adjust scenarios complexity, timing, and staffing needs.
- Implement Mini-Hospital exercise; run internal test scenario with students.
- Prepare for full operational launch.

Outcome: Validate training model VirtualLab and Table-top platform.

Phase 5 - Full Operational Capacity (Months 30-42)

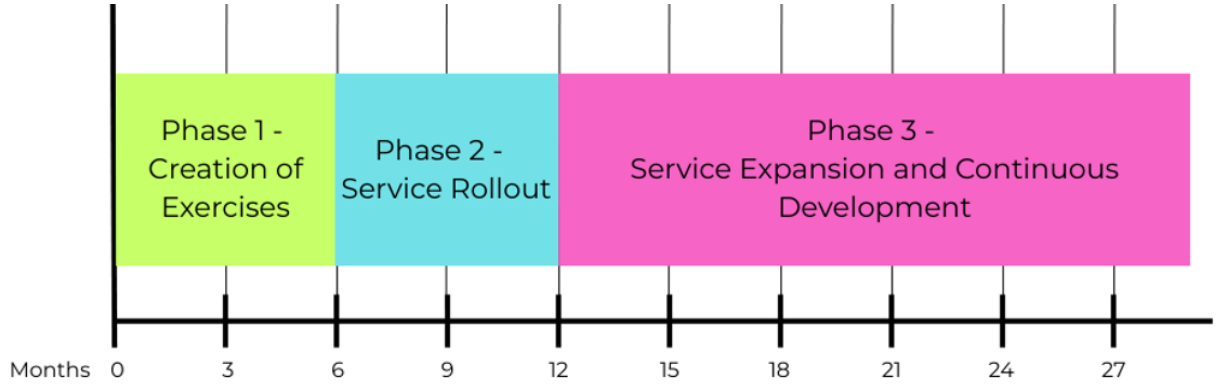
- Run 1-2 external Mini-Hospital pilots with selected organisations.
- Fully integrate Mini-Hospital into service portfolio
- Customisable scenarios available across all tracks.
- Active booking, payment, and reporting systems in place.

Outcome: Self-sustaining, nationally replicable social and healthcare cyber training environment.

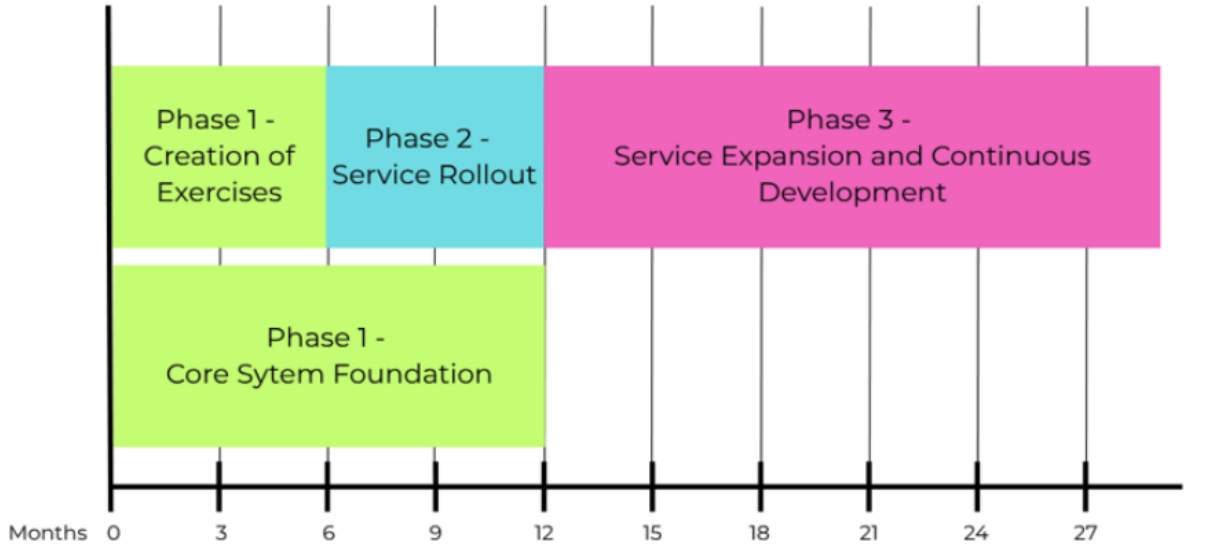
Parallel Activity Across All Platforms

- Continuous scenario development and dual-use adaptation between tracks.
- Marketing and outreach to new sectors.
- Student involvement in development, facilitation and RDI.

- Partnership building with agencies, vendors, and regional authorities.



Graphic 1: Timeline Table-Top platform.



Graphic 2: Timeline VirtualLab Cyber Simulation.

Graphic 3: Timeline Mini-Hospital.

Track A : VirtualLab Cyber Simulation

The VirtualLab Cyber Simulation delivers realistic cyber incident exercises via a secure, browser-based platform. It leverages prior EU project experience (CyberCare Kymi, Kyberturvan tulevaisuus Kymenlaaksossa) to meet the immediate training needs of social and healthcare SMEs, from solo practitioners to medium-sized providers.

Key Strengths:

- Accessible: No specialist hardware; runs in standard browsers.
- Scalable: Solo or multi-user training possible.
- Proven: Tested content adapted from real-world cyber incidents.

Phased Rollout and Milestones

Phase & Description	Milestones
Phase 1 – Core System Foundation (Months 0-6)	• Secure user authentication, role-based access control • Helpdesk & FAQ integrated • Two Tier 1 and 2 exercises developed • Internal security review completed • Outreach to private / public social and healthcare providers
Phase 2 – Service Rollout (Months 6-12)	• Launch first 4 exercises with automated feedback • Onboarding materials in plain language • First 10+ organisations trained
Phase 3 – Expansion & Continuous	• Tier 3 advanced scenarios added • On-campus training option enabled • Analytics dashboard operational

Development (months 12+)	• 4-6 new exercises added per year • First custom scenarios delivered

Impact by End of Year 3

- Catalogue: 15-20 exercises across tiers
- Organisations trained annually: 200+
- Repeat participation rate: ≥50%
- Resilience improvement: ≥30% from baseline

Track B: Table-Top Exercise Platform

The Table-Top Exercise Platform is the fastest to launch. The exercises provide strategic, decision-making focused cyber incident simulations for social and healthcare providers. They are designed to strengthen organisational readiness by simulating incident escalation – moving from internal disruption to media attention and service continuity challenges. These exercises require no special technical setup and are accessible via standard browser, making them ideal for solo entrepreneurs and SMEs.

Key strengths:

- No technical barriers: Accessible online, no setup required
- Scenario-driven: Decision-making under realistic pressure
- Regulatory alignment: Compliance with regulatory requirements for SMEs
- Dual-use content: Scenarios can be adapted for VirtualLab, reducing development costs

Phased Rollout and Milestones

Phase & Description	Milestones
Phase 1 – Core Scenario Development (Months 0-6)	• 2 existing micro-company scenarios finalised • 2 new scenarios for small companies developed • Incident escalation model designed • Automated reporting format created
Phase 2 – Service Rollout (Micro & Small) (Months 6-12)	• Launch for solo entrepreneurs, micro and small companies nationwide • 4 scenarios live (2 existing, 2 new) • Onboarding and facilitator guide complete • Fist customer trainings delivered
Phase 3 – Expansion to SMEs (Months 12-24)	• Add 4-6 new SME-focused scenarios • Include cross-sector specialisations (e.g. pharmacies, private clinics) • Enable joint sessions combining Table-Top & VirtualLab exercises
Phase 4 – Continuous Catalogue Growth (Months 24+)	• Add 4 new scenarios / year • Expand to sector specific themes (e.g. elder care, physiotherapy) • Maintain ≥80% satisfaction rate from participant feedback

Impact by End of Year 3

- Catalogue: 15-20 scenarios covering solo, micro, and SME
- Organisations trained annually: 200+
- Repeat participation rate: ≥50%
- Resilience improvement: ≥30% from baseline

Track C: Mini-Hospital Cyber Simulation

The Mini-Hospital Cyber Simulation delivers high-fidelity, on-site training for healthcare providers by replicating realistic cyber incidents within a controlled clinical environment.

This track develops from concept to full operational readiness in over 36-42 months, due to procurement requirements, infrastructure complexity, and the need for custom-built systems.

Key strength:

- Realistic: High-fidelity simulations replicate realistic cyber incidents in a live clinical setting
- Customisable: Scenarios and systems tailored to different healthcare organisations and threat levels
- Collaborative: Enables joint training for clinical, technical, and administrative teams in a shared environment

Phased Rollout and Milestones

Phase and Description	Milestones
Phase 1 – Planning (Months 0-6)	• System requirements defined (custom patient record system, observation rooms, automation trigger, etc) • Facility walkthroughs completed with stakeholders • Risk management plan and cost model finalised

Phase 2 – Procurement (Months 6-12)	• Servers, cabling, network segmentation, simulation software specified • Formal procurement launched
Phase 3 – Infrastructure Setup (Months 12-24)	• Physical infrastructure installed • Observations rooms operational • Simulated patient record system and patient monitoring integrated • Develop exercise script and walkthrough
Phase 4 – Pilot (Months 24-30)	• Implement Mini-Hospital exercise • Run internal test scenario with students • Prepare for full operational launch. • Technical and pedagogical feedback integrated • Scenario difficulty calibrated (technical disruption, automation triggers) • Staff training
Phase 5 – Full Operational Use (Months 30-42)	• Collect technical, pedagogical, and participant feedback. • Piloting with real companies • Adjust scenarios complexity, timing, and staffing needs. • Booking, onboarding, and analytic systems active • Custom simulations available for Tier 3 clients

Parallel Ongoing Activities

- Developing shared training / debriefing templates for Mini-Hospital, VirtualLab and Table-Top Platform
- Involve student projects in scenario development

- Build VirtualLab-compatible versions of Mini-Hospital scenarios for hybrid training
- Engage with hospitals, wellbeing counties, and agencies for partnership

Readiness Goal

True operational readiness: ~3-4 years from project start, assuming stable funding and no major delays. By completion, the Mini-Hospital will serve as a nationally replicable model for immersive healthcare cyber training.

Pilot and Evaluation Plan

This chapter outlines the structured pilot and evaluation process for each of the three training tracks. Rather than a one-size-fits-all approach, pilots are carefully aligned with the maturity and rollout timeline of each track. The goal is to ensure that every component functions as intended, meets the needs of its target audience, and produces measurable improvements in cybersecurity preparedness within the social and healthcare sector.

Track Specific Pilots and Objectives

Each training track undergoes a tailored pilot phase, designed to test core features, uncover usability issues, and gather feedback from real users in the field.

The Table-Top Exercises pilot will begin between months 6-9 of the project. It aims to test both the facilitation model and participant engagement during the exercises. These table-top simulations emphasis decision-making under pressure and are especially suited for solo entrepreneurs, micro and small companies. The pilot group will include a mix of two micro and 2 small social and healthcare providers.

The VirtualLab Cyber Simulation pilot will follow shortly after and run from months 9-12 of the project. Its focus is on validating the technical stability of the browser-based platform, ensuring user login and authentication flows work smoothly, and confirming that scenarios play out as designed with automated feedback and reporting. A small number of social and healthcare SMEs (2-3 organisations from Tier 1 and 2) will complete one or two exercises each, providing a realistic but manageable testbed.

The Mini-Hospital Cyber Simulation, due to its complexity and physical infrastructure requirements, will be piloted later in the project, between months 30 and 36. The primary objective is to assess the realism and usability of the simulation environment, including technical systems such as patient monitoring and automation triggers. The pilot will also evaluate interdisciplinary teamwork under simulated cyber incident conditions. Participants will include one medium-sized healthcare organisation or well-being county.

Participant Recruitment and Selection

Participants for the pilot phase will be recruited through direct outreach to organisations already active in the Kymenlaakso network, as well as through national partnerships with associations such as Suomen Yrittäjät or Regional Chambers of Commerce.

Educational institutions will also be involved, especially for student participation in scenario testing and feedback collection. Selection will aim for a diverse cross-section of organisations sizes and types – from solo entrepreneurs to larger SMEs – to ensure that results are broadly representative.

Criteria for selection include a demonstrated willingness to engage with the full pilot cycle, including pre- and post-training evaluations, and agreement to share anonymised operational insights that can inform future development. Efforts will

also be made to include participants from different regions to assess how well remote and hybrid model function in practice.

Evaluation Criteria and Success Metrics

To determine the effectiveness of each pilot, a combination of technical, educational, and experiential metrics will be used.

Technical reliability will be measured through system uptime (with a target of 99% or higher during sessions), the absence of critical error, and seamless integration of scenario automation and feedback tools.

Learning outcomes will be assessed using pre- and post-exercise questionnaires, with the expectation that at least 75% of participants report increased confidence in responding to cyber incidents. Additionally, evaluators will look for improved decision-making under pressure and stronger coordination among roles during simulation exercises.

Feedback from partner organisations will also be a key indicator of success. A target satisfaction rate of 80% or higher will be sought, alongside a 70% or greater intent to participate in future training rounds. Qualitative feedback will be used to identify specific improvements in scenario design and delivery.

Reporting and Iteration

Following each pilot phase, internal technical and pedagogical reviews will be conducted to refine scenarios, address bugs or usability issues, and enhance overall flow. This internal process includes detailed debriefs between engineers, pedagogues, and simulation facilitators.

Externally, quarterly reports will be prepared for funders and key stakeholders to communicate progress, pilot outcomes, and key learnings. At the end of each

development year, a consolidated impact report will be published, including data visualisation, anonymised participant quotes, and a roadmap for improvement. A public summary will also be made available to share national-level insights and demonstrate value to the sector.

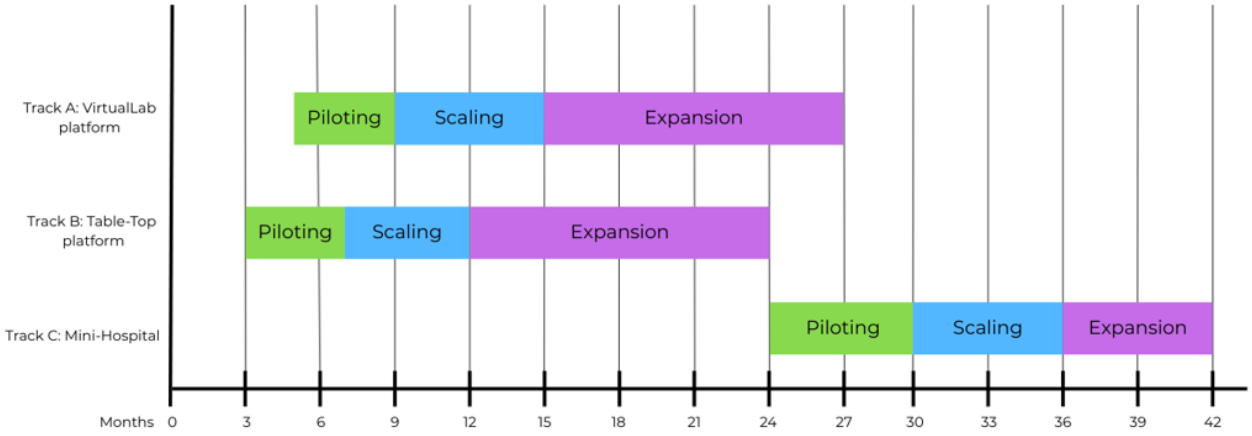
Timeline and Scaling Strategy

The rollout of the pilots follows the broader implementation timeline. In the first year (months 6-12), Track A and B will be piloted, refined, and used to finalise onboarding tools and the pricing model. This sets the stage for early adoption and feedback-led improvement.

During the second project year (months 12-24), pilots for VirtualLab and Table-Top will expand to reach new regions and user groups, aiming for 10-15 participating organisations. Data collected during this period will also support the integration of analytic tools and evaluation dashboards.

The Mini-Hospital will enter its pilot phase in the third year (months 24-30). Based on its outcomes, final adjustments will be made to technical systems, scenario pacing, and interdisciplinary facilitation models. By the end of year four, the full training ecosystem is expected to be ready for expansion.

Between months 36 and 42, all tracks will be scaled, with a target of at least 30 organisations actively participating. Hybrid training options – such as Mini-Hospital scenarios adapted for VirtualLab – will be introduced during this phase, further expanding reach and accessibility.



Graphic 4: Piloting, Scaling and Expansion Timeline all tracks.

Section 3: Personnel and Governance

Delivering a multi-track, technically complex training ecosystem requires a clear staffing plan and a governance structure that ensures quality, continuity, and accountability.

This section outlines the personnel requirements for each development and operational phase, including the roles needed to support VirtualLab, Table-Top and Mini-Hospital. It also describes how students can be integrated into scenario development and testing without replacing core staff.

In parallel, the governance model defines clear decision-making responsibilities across operational, technical, and strategic levels. A combination of internal leadership, sector partnerships, and expert advisory input ensures the project stays aligned with national regulations and sector-specific needs.

Personnel Requirements

Track A and B – VirtualLab and Table-Top Platform

Function	Role	Estimated FTE	Phase
Project Manager	Management, marketing	1.0	1-4
Technical Engineer	VirtualLab, integration and technical maintenance	1.0	1-3
Technical Engineer	Table-Top Platform, integration, technical maintenance	1.0	1-3

Technical Engineer	VirtualLab and Table-Top Platform technical maintenance	1.0	1-2
Cybersecurity Engineer (SOTE)	Scenario development, marketing	1.0	1-4
Simulation Pedagogue	Scenario Flow	0.3	1-4
Admin / Support	Scheduling, onboarding, marketing	0.5	1-3
Total		5.8	

Track C – Mini-Hospital Cyber Simulation

Technical Infrastructure and System Development

Function	Role	Estimated FTE	Phase
Project Manager	Management	1.0	1-5
Technical Lead	Infrastructure specification and integration	1.0	1-4
Content Developer	Scenario writing	1.0	3-5
Automation Specialist	Design and implementation control systems	1.0	1-4
Programmer	Patient record system, patient monitoring system, simulation triggers development and integration	2.0	1-4

Admin / Support	Scheduling, onboarding, logistics, supporting role	0.5	1-5
Marketing	Marketing	1.0	3-5
Total		7.5	

Student Participation

Pathway	Possible Contributions
Internship	Exercise development, scenario logic testing, virtual environment deployment, programming
Thesis	Designing training frameworks, automation feedback tools, user experience evaluation and tool
Project course	Scenario development Track A+B, threat simulation, design UX/UI elements

Student involvement is only in supporting roles, not substitution.

Project Governance

Effective governance is essential to deliver a technically complex, multi-track training concept on schedule, on budget, and to the required quality standards. The governance model combines clear leadership, technical authority, and external oversight to ensure that the project remains aligned with sector needs and national standards.

Governance Structure

The project is managed through three interconnected layers:

1. Core Management Team – day-to-day leadership, operational decision-making, and resource allocation.
2. Steering Group – strategic oversight, funding alignment, and risk management.
3. External Advisory Board – expert input from social and healthcare, cybersecurity, and educational stakeholders.

Core Management Team

The core management team is responsible for planning, executing, and quality control across all tracks.

Role	Responsibilities
Project Managers	Overall project delivery, budget tracking, final approvals on content and releases, reporting to Steering Group
Cyber Pedagogy & Learning Design Lead	Oversees scenario quality, learning objectives and pedagogical integration
Technical Leads	Approve technical architecture, supervise engineers, validate scenario deployment
Marketing	Maintains relationship with social and healthcare providers, manages onboarding and partner communications
Project Coordinator	Administrative support, scheduling, document control

Steering Group

The Steering Group provides strategic direction, ensures alignment with funding agreements, the institutions internal strategy, and monitors risks.

- Xamk senior management representative (chair)

- Project Manager (reporting)
- Lead representative from wellbeing county
- Representative from Finnish Cyber Security Center
- Representative from the private sector (SME social and healthcare provider)

Key Functions

- Approve major project milestones and budget allocations
- Monitor risk register and mitigation actions
- Facilitate cross-institutional cooperation

External Advisory Board

The external advisory board advises on sector relevance, scenario realism, and emerging threat trends.

Suggested members:

- Senior IT hospital / cybersecurity manager
- Clinical operations lead from wellbeing county
- SME representative (private sector)
- Cybersecurity academic expert
- Medical device specialist

Key Function:

- Review annual scenario catalogue for realism and sector alignment
- Provide insights on evolving threat landscapes
- Advise on integrating new technologies and best practices

- Strengthen links to national and international cyber resilience efforts

Decision-Making Process

1. Operational Decisions
    a. Made by Core Team
    b. Escalation to Steering Group for budget, scope, or risk issues beyond agreed thresholds
2. Technical Decisions
    a. Taken jointly by Technical Leads in consultation with relevant engineers and pedagogues
    b. Major architectural changes require Steering Group approval
3. Strategic and Funding Decisions
    a. Reserved for Steering Group
    b. Informed by external Advisory Board and Core Team recommendations

Section 4 : Financials and Sustainability

The long-term success of this concept depends on a financially sustainable model that allows for national reach, continuous scenario development, and affordable access for organisations of all sizes.

This section outlines the development and operational costs of each training track, along with a realistic revenue model based on tiered pricing and adoption projections. While external funding is essential during the initial build and pilot phases, the concept is designed to reach self-sufficiency by year 4.

Bu leveraging existing platforms, student involvement, and modular scenario reuse, the project minimises overhead while maximising sector-specific, but also at building scalable service model that can adapt to future training needs, regulatory changes, and sector expansion.

Detailed Budget and Cost Estimate

The budget is divided into two main components based on the training tracks:

a. Track A&B: VirtualLab Cyber Simulation and Table-Top exercise platform
b. Track C: Mini-Hospital Cyber Simulation (optional + one-time infrastructure investment)

Each track is split into personnel and non-personnel costs and aligned with the relevant project phases (e.g. development, rollout, testing, operations). Estimated Full-Time Equivalent (FTE) loads, and associated salaries are used to calculate personnel costs. Contingency buffers are included to account for uncertainty.

Revenue Model and Sustainability Plan

The sustainability of the concept relies on a realistic pricing model, phased market adaptation, and a bundle training offer that includes both VirtualLab Cyber Simulation and the Table-Top exercises.

This section outlines tiers, market size assumptions, forecasted revenue, and a break-even analysis across the first four years of operation.

1. Pricing Structure (per organisation / per year)

This is sold as a bundle: VirtualLab and Table-Top exercise based on a shared storyline. This model improves learning outcomes while reducing development effort.

Organisation	Bundle Prize (€)
Solo entrepreneurs	80
1-5 employees	100
6-10 employees	180
11-20 employees	250
21-50 employees	400

Bundle pricing is 20-25% cheaper than purchasing tracks separately, while still maximising revenue.

2. Market Size and Adaptation Assumption

Target Group: Social and Healthcare organisations across Finland

Total addressable organisations: ~15 000

Assumed yearly usage per organisation: 1 VirtualLab + 1 Table-Top

Adaption Ramp (Years 1-4)

Year	Solo/Micro Adaption	SME Adaption
1	1 %	0.5%
2	3 %	1 %
3	5 %	2 %
4	7 %	3 %

3. Revenue Forecast Tracks A&B

Year	Solo/Micro	Avg. Price (€)	Revenue (€)	SME Orgs	Avg. Price (€)	Revenue (€)
1	50	120	3 780	15	325	4 875
2	200	120	24 000	30	325	9 750
3	600	120	72 000	60	325	19 500
4	840	120	100 800	90	325	29 250

Weighted average prices reflect organisational distribution and tiered pricing.

4. Break-even Analysis

Estimated operational and development costs (content, technical, support) after year 4: ~130 000 € / year

Year	Cumulative Revenue (€)
1	19 275
2	52 950
3	91 500
4	130 050

Break-even scenarios:

- With external funding for Year 1-2: Self-sustaining after year 4.

- Without funding: Break-even reached in ~6 years, assuming flat adoption ramp.

Sustainability Summary

- Pricing is accessible for solo and small providers, while scaled appropriately for SMEs.
- Adoption ramp is realistic, based on sector-wide digital maturity.
- The bundled approach maximises cost-efficiency in both development and delivery.
- The model becomes sustainable within four years under conservative assumptions – and earlier if uptake exceeds projections.

Funding Opportunities and Strategies

Ensuring the long-term success and national impact of the training ecosystem requires a multi-source funding approach that supports both early-stage development and sustained operations. This section outlines targeted funding opportunities, aligned with national and EU priorities, and details how different financing sources can support specific phases — ranging from infrastructure and content development to scale-up, replication, and internationalisation.

Marketing and Communication Strategy

Effective communication is essential to ensure that the training ecosystem reaches its target audiences—especially small and medium-sized healthcare providers (SMEs) and wellbeing services counties (HVA). The strategy focuses on building awareness, trust, and engagement through tailored channels and

partnerships, with a particular emphasis on early-stage outreach during the development and pilot phases.

To reach SMEs, the project will utilise sector-specific communication channels, including newsletters, webinars, and targeted social media campaigns through healthcare associations and cybersecurity networks. Collaborations with key regional actors—such as development agencies, university networks, and chambers of commerce—will serve as multipliers, extending reach and helping to identify pilot clients and early adopters across different regions.

Visibility will also be maintained through active participation in national events that bring together stakeholders from both cybersecurity and healthcare sectors. These may include conferences, trade fairs, and government-hosted innovation showcases. The project team will contribute to panels, host workshops, and present pilot results to attract attention and build credibility.

Early outreach will focus on identifying forward-looking organisations—especially among SMEs and HVA units—that are willing to test new training methods and co-develop the first scenarios. These early adopters not only help validate the training tools but also serve as ambassadors to promote adoption within their networks, contributing to organic growth and sector-wide impact.

Funding Target

The funding sought will directly support the creation of a nationally scalable, sector-specific cyber training ecosystem. Key targets for investment are aligned with the most resource-intensive and strategically critical components of the project's early stages.

A primary focus is the hardware infrastructure required to bring the Mini-Hospital simulation environment to life. This includes a dedicated simulation layer with realistic clinical setups, segmented networks for controlled cyber

incidents, and specialised, non-standard servers capable of supporting complex, automation-driven training scenarios.

In parallel, custom software development is essential to build immersive, healthcare-specific cyber scenarios within the Mini-Hospital. This includes the development of a simulated patient record system, integration with monitoring devices, and the creation of incident automation tools that allow for high-fidelity, interdisciplinary training.

Funding will also support the recruitment and retention of key personnel during the intensive 30-month development period. This includes scenario developers, technical engineers, cybersecurity specialists, and pedagogical experts—each vital to ensuring that the training content is realistic, functional, and aligned with sector needs.

Finally, the project aims to significantly expand the VirtualLab scenario catalogue, increasing accessibility for micro and small healthcare organisations across Finland. The goal is to provide browser-based training modules that lower entry barriers while maintaining pedagogical impact. Ensuring the availability and quality of these modules is central to the project's scalability and long-term sustainability.

Potential Funding Sources

Funder	Rationale
Regional Council / ELY-Keskus	Supports digitalisation of SMEs, regional innovation, and NIS2 preparedness; aligns with regional cybersecurity capacity-building goals

Business Finland	Innovation in healthcare infrastructure and cybersecurity services
Finnish Ministry of Social Affairs and Health (STM)	Strategic fit with national social and healthcare system resilience, especially NIS2 implementation and preparedness development.
EU Resilience Funds / Digital Europe / Horizon Europe	Provides support for simulation infrastructure, critical sector digital security, and cross-border training environments; enables scalable model replication.
ESR+ (European Social Fund Plus)	Focused on workforce development, continuous learning, and strengthening the interface between education providers and employers in critical sectors.

Section 5: Risk and Compliance

This concept combines multiple disciplines—healthcare simulation, cybersecurity, IT infrastructure, and public-sector training—into one national-scale service. While the benefits are significant, so are the risks. Technical delays, procurement requirements, interdisciplinary coordination, and funding uncertainties must all be actively managed to ensure timely delivery and long-term viability.

This section provides a clear, transparent overview of the project's risks and compliance measures. The challenges are presented in a structured risk matrix that rates likelihood and impact, and each risk is linked to specific mitigation actions and responsible persons. Financial and operational fallback scenarios are also included to demonstrate resilience.

Risk Matrix Overview

To manage the complexity of this multi-track concept, we apply a structured risk assessment approach using a Risk Matrix. The matrix provides a transparent overview of the key risks that may affect the successful development, rollout, and sustainability of the training model.

Each identified risk is assessed along two axes:

- Likelihood – The estimated probability that the risk will materialise during the project.
- Impact – The severity of the consequences should this risk occur.

Both are rated on three-point scale:

Level	Description
Low	Unlikely to occur or would have minimal consequences.
Medium	Could occur under some conditions; manageable impact with disruption.
High	Likely to occur; significant impact on project schedule, quality, or scope.

Each risk is also assigned a mitigation strategy to reduce the likelihood or impact.

The risk matrix is meant to be updated regularly during the project, particularly during major decision points.

Challenges and Risks

Risk	Likelihood	Impact	Mitigation Strategy
Recruitment Challenges for Core Personnel – The project requires highly skilled staff with experience in cybersecurity, simulation, and healthcare. Limited availability of such experts in Finland may delay hiring and increase workload on existing staff.	High	High	Begin recruitment early; involve students early; establish partnerships with universities and hospital IT units; maintain a flexible hiring structure to attract talent.

Lack of Healthcare-Experienced Scenario Developers – Limited availability of personnel with both clinical background and cybersecurity knowledge. Without authentic insight into hospital processes, exercises may fail to reflect real-world conditions.	High	High	Co-develop exercises with HVA clinical staff; establish an advisory group for scenario validation; use joint student projects to strengthen internal know-how.
Operational Overload During Intensive Phases – During peak development months, the same staff may be responsible for technical, pedagogical, and coordination tasks, leading to burnout or quality issues.	Medium	High	Implement workload mapping; secure temporary technical support; distribute responsibilities between tracks; prioritise tasks and avoid overlapping milestones.
Loss of Key Staff During Development – Departure or unavailability of critical personnel (technical lead, pedagogue, or content developer) may	Medium	High	Maintain detailed documentation; introduce handover procedures; cross-train backup staff; provide retention incentives for key team members.

cause knowledge gaps or rework.			
Technical System Integration Failures – The complexity of linking patient record systems, monitoring devices, and automation tools may result in malfunctions or data conflicts during simulation.	Medium	High	Conduct phased testing and integration reviews; retain external experts for critical connections; use isolated test environments before live deployment.
Funding Discontinuity or Reduction – Delays or changes in external funding may interrupt ongoing development or limit the Mini-Hospital build.	Medium	High	Diversify funding sources (EU, STM, Sitra, regional); maintain project reserves; prioritise VirtualLab deliverables to show progress and retain funder confidence.
Low Engagement from Target Organisations – SMEs or HVAs may not allocate time or budget to participate in pilot training, slowing national adoption.	Medium	High	Use strong marketing campaigns through regional networks; offer subsidised pilot sessions; publish impact results to build trust; align scenarios with NIS2 obligations.
Budget Overruns Due to Equipment and Software Costs – Inflation, vendor price changes, or underestimated	Medium	Medium	Maintain a 10–15% contingency fund; conduct early vendor negotiations; phase purchases by track;

integration needs could exceed initial cost forecasts.			prioritise critical components first.
Regulatory or Policy Changes Affect Project Requirements – Adjustments to NIS2, healthcare IT standards, or public procurement laws may necessitate technical or procedural changes.	Low	Medium	Monitor regulatory updates through STM and Kyberturvallisuuskeskus; maintain adaptable infrastructure; ensure flexibility in system documentation.
Mismatch Between Technical Capabilities and Training Needs – If the simulation environment lacks the right triggers, device behaviour, or automation features, the exercises may not sufficiently reflect real-world healthcare workflows or cybersecurity pressure points.	Medium	High	Involve end-users (clinical staff and IT) in early scenario design; run technical walkthroughs before pilots; iterate based on feedback; build simulation flexibility into infrastructure choices.

Exercise

A scenario-based cybersecurity exercise was designed to simulate a cyber crisis in a hospital setting, engaging multidisciplinary teams in realistic and time-critical decision-making. Developed as part of the CyberCare Kymi project, the exercise reflects the complex and interdependent nature of modern healthcare environments, where digital disruptions can directly affect patient safety and continuity of care.

The exercise serves as a training platform to strengthen operational preparedness, information security awareness, and coordination between clinical, technical, and managerial roles. Participants are immersed in a simulated incident involving critical system failures, requiring them to navigate disruptions, apply existing security protocols, and ensure safe care delivery through alternative procedures.

By aligning with real-world threats and sector-specific requirements, the exercise fosters organisational learning, highlights critical vulnerabilities, and promotes a proactive security culture across the healthcare system.

The exercise was designed and developed by Sitowise.

CyberStorm in the Hospital – cyber security training

Technical-Operational Exercise in a Hospital Environment

This chapter describes a cybersecurity exercise designed for a hospital setting as part of the CyberCare Kymi project. The exercise was developed as a multi-player group scenario. The term SOC will be used hereafter to refer to the Security Operation Center.

Background and Objectives

The CyberCare Kymi project supports social and healthcare organisations in the Kymenlaakso region in strengthening their cyber and information security capabilities, preparing for continuity of operations, and practicing recovery strategies. The goal of the exercise is to enhance cyber crisis readiness and increase participants' understanding within their familiar hospital work environment.

This work was implemented as an extension of the previous "CyberCare Kymi – Technical-Operational Cyber Exercises 2024" project and adheres to the principles outlined in that project's final report.

Storytelling and Scenario Progression

Organisational Background and Initial Setting

The scenario is based in a typical hospital organisation that is part of the Kymenlaakso wellbeing services county. The organisation has prepared for current cybersecurity threats by creating an information security plan and implementing measures to ensure patient safety.

Beginning of the Story and Turning Point

“The organisation has recently undergone changes, and now the entire team is working in new premises for the first time. Some information systems have also changed, but people are learning to use them. Fortunately, there are familiar faces around.”

Management and IT have gathered to review and improve the information security plan. Meanwhile, nurses and reception staff are carrying out their normal daily tasks at their workstations or on the wards.

As the management and IT teams begin reviewing the security plan, the first signs of disruption appear. A cyberattack targets the hospital’s information systems, affecting a critical patient information system (Scenario 1). Just as the situation appears to stabilise, a second disruption unexpectedly affects the email service (Scenario 2). The situation escalates when the systems do not function properly after the attack, forcing staff to switch to manual procedures to ensure patient safety.

Scenario 2 is considered optional depending on how much time is spent on Scenario 1. The total time allocated for the exercise is approximately 4 hours, with additional time reserved for the debriefing session afterwards.

Objective, Conclusion, and Evaluation of the Exercise

The main objective of the exercise is to improve participants' ability to operate during exceptional situations where hospital information systems are under cyberattack. Participants act in their professional roles, identify development areas in their own preparedness, and strengthen their knowledge in leadership, decision-making, communication, and clinical operations during a disruption.

The key priorities are to:

- Ensure the continuity of hospital operations

- Guarantee patient safety
- Restore the functionality of information systems

Success is measured by how effectively leadership, crisis communication, technical response, and continuity of clinical operations work together, and how the organisation manages the controlled recovery of critical services.

Metrics for Evaluating Success:

- Compliance with the organisation's information security plan (and identification of any gaps)
- Clarity and effectiveness of crisis communication
- Patient safety (execution of manual procedures and response time)
- Recovery of systems and services

Key Events (MITRE MSEL)

Orientation

Player orientation and distribution of the incident response plan. At the same time, players are introduced to the initial narrative setting. The introduction is given by a WHITE cell facilitator, who takes on the role of an IT consultant during the orientation. They describe the players' operating environment and express concern about recent changes in the cyber threat landscape, based on what they've read in newspapers and seen on the news.

Assumptions for the orientation:
The WHITE cell produces media material for the media play component, illustrating the cyber threat landscape. This material also includes news related to the social and healthcare sector, including cyberattacks and their consequences.

Exercise Assumptions

1. The participating organisation has its own information security plan, which is followed during the exercise.
2. Since the technical environment of the exercise differs slightly from the organisation's actual setup, a supplementary document is provided to participants. This document includes:

- Contact information for support services: SOC and electronic health record system provider. The system vendor is responsible for both the patient information system and email system.
- The organisation's primary communication channel during incidents is email, with SMS as a backup.
- In the event of a disruption affecting the Kanta services, a disruption report is to be submitted to Kela via the Simternet form. Alternatively, Kela's support can be contacted by phone.
- Emergencies are reported to the Emergency Response Centre (HäKe) via a phone call. WHITE

3. Nurses are also provided with a printed contact sheet, including:
   - IT support phone number and email
   - Emergency Response Centre phone number (HäKe)
   - Taxi phone number
4. The number of patients on wards scales according to the number of participating nurses from the organisation. For example, a large number of participants enables a constant flow of new patients arriving at the reception area.
5. The exercise will require paper-based forms due to system disruptions.
6. The system disruption should last long enough for all players in their respective roles to engage as expected.
7. Preparation is required for participation in the exercise.

Scenario 1	Subject: Hospitals Electronic Health Record (EHR) System			
Relative Time	Inject	Description	Roles	Expected Action
T-00:00	Security Plan Treatment Case: Sprained ancle Treatment Case: ICU patient	Management BLUE and IT BLUE receive the cybersecurity plan and exercise-specific attachment.	Management BLUE IT BLUE Patient (ICU) WHITE Patient (ankle sprain) WHITE	Management and IT BLUE review the plan and attachment. Nurses BLUE begin treatment procedures.

T+00:10	Attack on patient information system	Attacker RED carries out an attack on the patient information system, deletes the system's log and configuration files from the server, and brings the system down.	Attacker RED	System becomes unavailable to users.
T+00:10	A patient with severe headache arrives.	WHITE plays the role of a patient at the reception.	New Patient WHITE Reception Nurse BLUE	The reception nurse asks the patient about the reason for their visit. The nurse attempts to open the patient information system.
T+00:15	Main view of client system fails to load	The nurse at the reception desk cannot access the client/patient information system to check the details of the arriving patient.	Nurse BLUE Head Nurse BLUE	The nurse at the reception desk observes that the client/patient information system is in a disrupted state. Nurse BLUE submits a disruption report to IT BLUE in accordance with the information security plan.
T+00:25	System failure report sent to IT	IT BLUE receives a disruption notification regarding the client/patient information system by email.	IT BLUE Management BLUE Kela Support WHITE	IT BLUE begins investigating the disruption in accordance with the incident process defined in the information security plan. IT BLUE informs BLUE Management

				about the disruption. IT BLUE investigates whether the disruption in the client/patient information system is local or external. The problem is local. IT BLUE submits a disruption notification to Kela using the disruption form or by calling Kela Support (WHITE). IT BLUE requests logs related to the client/patient information system from SOC (GREEN), including network traffic, server, and application logs.
T+00:55	Management receives system failure update	Management receives a disruption incident report from IT regarding the client/patient information system, either verbally or by email.	Management BLUE	Management BLUE is involved in investigating the situation in accordance with the incident process, particularly from the perspective of communications and with regard to what must be taken into account from the hospital's point of view. Actions: convening of the crisis team.

				Notify the Emergency Response Centre (by phone) that the hospital cannot receive patients.
T+01:15	Management informs the reception and the wards about the transfers of urgent patients.	The reception cannot accept patients. Urgent patients begin to be transferred from the wards to other locations for treatment.	Management BLUE	Management informs that patient safety must be ensured and that wards will switch to manual, paper-based documentation of patient and care information. Management instructs that patients currently on the wards will have to be transferred to another location for treatment (an intensive care unit patient).
T+01:25	The reception receives a notice from Management. The ward receives a notice from Management. The intensive care unit	The emergency department is closed because the electronic patient health record system is not functioning. On the ward, patients who require transfer are assessed, and treatment is continued if there is no need for transfer. In the intensive care unit,	Reception Nurse BLUE Head Nurse BLUE	The patient who arrives at the reception has to be redirected to another location. The nurse orders a taxi to transport the patient to the health center (ankle sprain). The patient with a headache is transferred by ambulance to another hospital. The nurse organizes the

	receives a notice from Managemen t.	planning of the patient's transfer is initiated.		transfer to another location. Patients are transferred from the intensive care unit. The nurse organizes both the patient transfer and the transfer of information to the new place of care. Matters related to treatment and transfers are documented on paper.
T+01:30	SOC sends logs to IT	SOC GREEN sends system logs via email to IT BLUE.	SOC GREEN IT BLUE	IT BLUE identifies attack path (via compromised service provider credentials).
T+02:15	IT instructs the EHR system provider to restore the client/patient information system and to close the attack vector.	IT BLUE instructs EHR system provider GREEN to recover the system and close the breach.	IT BLUE EHR system provider GREEN	EHR system provider GREEN closes the attack vector and restores the patient information system. EHR system provider GREEN informs IT BLUE that the system has been restored.
T+02:45	The EHR system provider informs IT that the system has been restored.	EHR system provider GREEN confirms to IT BLUE.	IT BLUE EHR system provider GREEN	IT BLUE informs management BLUE and healthcare staff that the incident is over. IT BLUE notifies EHR support (form in Simternet).

T+02:50	IT informs Management that the system has been restored to operation. IT informs the healthcare staff that the system has returned to normal.	IT BLUE notifies management BLUE that the system is operational. IT BLUE informs staff BLUE, that the system is operational.	IT BLUE Management BLUE Head Nurse BLUE	Management BLUE considers wider comms: staff, media, CERT-FI, authorities. Retroactive data entry begins. Evaluation begins, have EHRs been exfiltrated? (Notify Data Protection Commissioner) Valvira. Management plans police report. The head nurse plans the transfer from paper EHR to the digital EHR.
Scenario 2 (optional)	Subject: Hospital Email System (Incident Situation)			
Relative Time	Inject	Description	Roles	Expected Action
T+03:15	SMS to head nurse: "Work shift schedules have not arrived."	Head nurse BLUE receives SMS from off-duty nurse WHITE stating that work schedules have not arrived via email.	Head Nurse BLUE Off-duty Nurse WHITE	Head nurse BLUE attempts to access the webmail system, which does not load. Notifies IT BLUE via SMS.
T+03:20	SMS from head nurse to IT	Head nurse BLUE informs IT BLUE of the suspected issue in the email system.	IT BLUE Head Nurse BLUE	IT BLUE verifies the issue with the email system. Once confirmed, verbally notifies Management BLUE.

T+03:25	IT verbally informs management about email system disruption	IT BLUE verbally informs management BLUE about email system disruption. The email system problem is confirmed.	IT BLUE Management BLUE	Management BLUE plans internal and external communication related to the disruption.
T+03:30	IT calls system provider	IT BLUE contacts the email provider to investigate the email system incident. The email provider confirms a temporary disruption that will be resolved in 30 minutes.	IT BLUE Email Provider GREEN	IT BLUE and Management BLUE evaluate all services impacted by the disruption.
T+04:00	SMS from provider to IT: issue resolved	The email provider GREEN restores the email system and notifies IT BLUE.	Email Provider GREEN IT BLUE	IT BLUE informs Management BLUE verbally and notifies staff via SMS that the issue is resolved.

Exercise Progress Monitoring

During the exercise, the White Team requires situational awareness to monitor progress and assess the players' reactions, learning, and ability to navigate the scenario. The players' ability to move through the scenario directly impacts whether the pre-planned storyline and technical injects can be executed.

The exercise is monitored using the following assets:

System	Configuration / Monitoring Purpose
White Team Email System	Alert triggered when a specific player or player team sends an email to the White Team.
Blue Team Email System	Operational system targeted by the attack. Its state must be monitorable by the White Team.
Mobile Phones (multiple): · IT / Management BLUE · Head Nurse BLUE · Cybersecurity students RED / GREEN / WHITE	No specific configuration. Note: SMS messages cannot be tracked unless a dedicated app (like an SMS simulator) is used.
Access Management System in Player Environments	Logging of access events to Green Team-controlled monitoring area. Allows the White Team to confirm whether the player has accessed the game environment or confirmed system recovery.
Network Traffic Monitoring between Client and Server (HTTP)	Logging and access to traffic events in the Green Team-controlled area. Allows the White Team to confirm that the player is following the expected path and completing scenario tasks.
Kela Incident Notification Form Kela Incident Notification Website (Simternet) WHITE	Submission, tracking, and management of incident notifications. Kela also uses this system to report its own service outages.
Patient and Client Information Systems and related data/users in Player Environments	Logging of activity in patient and client information systems and their databases to the Green Team area. Enables the White Team to verify scenario progress and task completion.
Red Team foothold tool (RAT) or reverse shell in Player Environment	Red Team collects evidence of foothold using scripts (e.g., confirmation of access). This data is forwarded to the Green Team-controlled area and accessible to Red and White Teams.

Concept Conclusion

This concept began with a focus on creating a physical Mini-Hospital Cyber Simulation environment—an immersive training space designed to simulate technical disruptions in clinical settings. However, as the project matured, two additional solutions emerged as more flexible, scalable, and cost-effective: the VirtualLab and the Table-Top platform.

While the Mini-Hospital concept offers pedagogical depth and realism, its long-term viability is constrained by high infrastructure costs, staffing needs, and the limited number of healthcare providers within reach who could consistently benefit from on-site training. Based on a sustainability threshold of approximately 30–40 participating organisations per year, maintaining such a facility cannot be justified without major ongoing subsidies or national-level institutional backing.

During the development process, it became clear that VirtualLab and the Table-Top platform provide similar training outcomes for most target groups, with significantly lower costs and broader accessibility. By restructuring the Mini-Hospital scenario as a VirtualLab-based exercise—delivered through portable laptops in existing rooms—the concept retains its pedagogical strength while eliminating the need for physical retrofitting, observer room integration, and custom infrastructure.

For this shift to succeed, VirtualLab must be stable, intuitive, and well-supported, capable of handling a diverse range of scenario-based exercises across technical and non-technical tracks. It will require focused investment in platform development, automation, and ongoing technical maintenance.

Recommendation

Redirect development priorities and funding toward the VirtualLab and Table-Top tracks, which emerged as stronger, more adaptable pillars of the training model. They support broader rollout, lower operational risk, and offer the flexibility to grow into national and international training ecosystems—while still honouring the original vision of preparing the social and healthcare sector for future cyber threats.

References and Sources

Abad, A. H., Corbiaux, S., Ifigeneia, L., Theocharidou, M. 2023. Enisa Threat Landscape: Health Sector. European Union Agency for Cybersecurity. PDF-document. Available at: https://www.enisa.europa.eu/publications/health-threat-landscape [Accessed 8.2.2025]

Directive (EU) 2022/2555 of the European Parliament and of the Council

Advanced and unique cyber range. Jyvsectec by jamk. Website. Available at: https://jyvsectec.fi/en/realistic-global-cyber-environment/ [Accessed 3.11.2025]

Rantakoski, T. 2023. Sote-yritykset tehostaisivat hyvinvointialueiden palveluja – Ministeri: Erikokoisia toimijoita tarvitaan. Yrittäjät. Article. Available at: https://www.yrittajat.fi/uutiset/sote-yritykset-tehostaisivat-hyvinvointialueiden-palveluja-ministeri-erikokoisia-toimijoita-tarvitaan/ [Accessed 2.6.2025]

Cybersecurity Act (NIS2). Valvira. WWW-document. Available at: https://valvira.fi/en/healthcare-and-social-welfare/cybersecurity-act [Accessed 3.11.2025]