TRAFICOM
Finnish Transport and Communications Agency

NCC-FI
FINLAND NATIONAL COORDINATION CENTRE FOR CYBERSECURITY

Impact evaluation of the financial support provided by the National Co-ordination Centre Finland (NCC-FI)

Evaluation Report

Heidi Uitto
Kimmo Halme
Vesa Salminen
Timo Kotilainen

Co-funded by the European Union

Traficom Research Reports
Traficomin tutkimuksia ja selvityksiä
Traficoms forskningsrapporter och utredningar

04/2025

TRAFICOM
Liikenne- ja viestintävirasto

Julkaisupäivämäärä
17.1.2025

Julkaisun nimi
Kansallisen koordinointikeskuksen (NCC-FI) rahoitustuen vaikuttavuusarviointi

Tekijät
Heidi Uitto (4Front Oy), Kimmo Halme (4Front Oy), Vesa Salminen (4Front Oy) & Timo Kotilainen (Kasin Consulting Oy)

Toimeksiantaja ja asettamispäivämäärä
Liikenne- ja viestintävirasto Traficom 27.9.2024

Julkaisusarjan nimi ja numero
Traficomin tutkimuksia ja selvityksiä 04/2025
ISSN (verkkojulkaisu) 2669-8781
ISBN (verkkojulkaisu) 978-952-311-952-9

Asiasanat
Modernit kyber- ja tietoturvaratkaisut, käyttöönotto, pk-yritykset, rahoitustuki, kyberturvallisuuskapasiteetti

Tiivistelmä
Arvioinnissa tarkasteltiin Liikenne- ja viestintäviraston Kyberturvallisuuskeskuksen Kansallisen koordinointikeskuksen (NCC-FI) pk-yrityksille suunnatun modernien tieto- ja kyberturvaratkaisujen ja innovaatioiden käyttöönottoon tarkoitetun rahoitustuen suoria ja epäsuoria vaikutuksia. Arvioinnin keskeisiä menetelmiä ja tietolähteitä olivat projektisuunnitelmien, hakemusten ja datan analysointi, tuensaajille suunnattu kysely, asiantuntijahaastattelut, kirjallisuuskatsaus ja validointityöpaja.
Arviointi toteaa, että taloudellinen tuki on ollut tarkoituksen mukainen, ja sen suorat vaikutukset tuensaajiin voidaan katsoa suuriksi. Lähes kaikki rahoitusta saaneet projektit (95 %) ilmoittivat käyttöönottaneensa teknologioita onnistuneesti ja saavuttaneensa projektinsa tavoitteet. Yritykset raportoivat myös lisääntyneestä resilienssistä kyberhyökkäyksiä vastaan.
Epäsuorien vaikutusten osalta arvioinnissa tarkasteltiin vaikutuksia kyberturvamarkkinoihin ja kansalliseen kyberturvakapasiteettiin yleisesti. Taloudellinen tuki on synnyttänyt IT-palveluiden kysyntää noin 0,9 miljoonan euron arvosta. Palveluiden toimittajat olivat pääasiassa suomalaisia yrityksiä. Hankitut teknologiset ratkaisut puolestaan olivat pääosin kansainvälisten suuryritysten tarjoamia. Suhteellisuuden ja tarkoituksenmukaisuuden osalta näyttää selvältä, että tuen määrä (2 miljoonaa euroa) on rajallinen kansallisiin tarpeisiin nähden. Tuen määrän huomioon ottaen, on sopivaa, että sitä myönnetään kohdennetusti ja kannustimena. Avustuksen enimmäismäärä (60 000 euroa) voisi olla yhtä tehokas hieman pienemmässä muodossa (esimerkiksi 20 000 euroa), jolloin voitaisiin jakaa enemmän avustuksia.
Arvioinnissa suositellaan, että yritysten kyberturvallisuuden parantamiseen tarkoitettua tukea tulisi jatkaa kansallisesti. Vaikuttavuutta voitaisiin lisätä pienentämällä yksittäisten avustusten kokoa ja laajentamalla samalla myönnettyjen avustusten määrää. Lisäksi välineen tulisi tukea kokonaisvaltaista lähestymistapaa kyberturvallisuuteen ja kannustaa yrityksiä toteuttamaan käyttöönoton ohella muita toimia, esim. koulutus ja tiedonvaihto muiden yritysten kanssa. Vaikuttavuutta voitaisiin tehostaa täydentämällä rahoitustukea ei-taloudellisella tuella, kuten teknisellä ohjauksella ja hyvien (prosessien) käytäntöjen jakamisella.

Yhteyshenkilö
Annalotta Saarikoski

Raportin kieli
Englanti

Luottamuksellisuus
Julkinen

Kokonaissivumäärä
57

Jakaja
Liikenne- ja viestintävirasto Traficom

Kustantaja
Liikenne- ja viestintävirasto Traficom

TRAFICOM
Transport- och kommunikationsverket

Utgivningsdatum
17.1.2025

Publikation
Effektutvärdering av det finansieringsstöd som tillhandahålls av Nationella samordningscentrumet (NCC-FI)

Författare
Heidi Uitto (4Front Oy), Kimmo Halme (4Front Oy), Vesa Salminen (4Front Oy) & Timo Kotilainen (Kasin Consulting Oy)

Tillsatt av och datum
Transport- och kommunikationsverket Traficom, 27.9.2024

Publikationsseriens namn och nummer
Traficoms forskningsrapporter och utredningar 04/2024
ISSN (elektronisk publikation) 2669-8781
ISBN (elektronisk publikation) 978-952-311-952-9

Ämnesord
toppmoderna informations- och cybersäkerhetslösningar, SMF, finansieringsstöd, nationella cybersäkerhetskapaciteten

Sammandrag
Utvärderingen bedömde de direkta och indirekta effekterna av finansieringsstödet till SMF för att implementera toppmoderna informations- och cybersäkerhetslösningar och innovationer som beviljats av det Nationella samordningscentrumet vid Transport- och kommunikationsverkets Cybersäkerhetscenter. De huvudsakliga metoderna och datakällorna i utvärderingen var analys av projektplaner, ansökningar och data, enkäter riktade till stödmottagare, expertintervjuer, litteraturgenomgång och en valideringsworkshop.
När det gäller direkta effekter för stödmottagarna fann utvärderingen att det ekonomiska stödet har uppfyllt sitt syfte väl och att dess direkta påverkan kan anses vara hög. Nästan alla projekt (95 %) uppgav att de framgångsrikt har implementerat sina tekniska uppgraderingar och uppnått sina projektmål. Företagen rapporterade också ökad motståndskraft mot cyberattacker.
När det gäller indirekta effekter undersöktes inverkan på cybersäkerhetsmarknaden och den nationella cybersäkerhetskapaciteten i stort. Det ekonomiska stödet har genererat ytterligare efterfrågan på IT-tjänster till ett värde av cirka 0,9 miljoner euro. Dessa tjänster tillhandahölls huvudsakligen av finländska företag. De tekniska lösningar som köptes in tillhandahölls dock främst av stora internationella företag. Med avseende på proportionalitet och ändamålsenlighet verkar det tydligt att volymen (2 miljoner euro) är begränsad med hänsyn till nationella behov. Därför är volymen lämplig som ett riktat stöd och en incitamentsmekanism för att adressera vissa identifierade utmaningar. Stödets maximala storlek (60 000 euro) skulle kunna vara lika effektiv i något mindre omfattning (till exempel 20 000 euro), vilket skulle möjliggöra fler utdelade bidrag.
Utvärderingen rekommenderar att ytterligare stöd till företag för att uppgradera sin cybersäkerhet bör säkerställas. Effektiviteten kan ökas genom att minska storleken på individuella bidrag samtidigt som antalet utdelade bidrag utökas. Instrumentet bör också stödja ett holistiskt angreppssätt på cybersäkerhet och uppmuntra företag att vidta åtgärder utöver införandet av teknologi. Dessutom bör ekonomiskt stöd kompletteras med icke-ekonomiskt stöd, såsom teknisk vägledning och delning av god (process-) praxis för att ytterligare förbättra effektiviteten.

Kontaktperson
Annalotta Saarikoski

Språki
Engelska

Sekretessgrad
Offentlig

Sidonantal
57

Distribution
Transport- och kommunikationsverket Traficom

Förlag
Transport- och kommunikationsverket Traficom

TRAFICOM
Finnish Transport and Communications Agency

Date of publication
17th of January 2025

Title of publication
Impact evaluation of the financial support provided by the National Coordination Centre Finland (NCC-FI)

Author (s)
Heidi Uitto (4Front Oy), Kimmo Halme (4Front Oy), Vesa Salminen (4Front Oy) & Timo Kotilainen (Kasin Consulting Oy)

Commissioned by, date
Finnish Transport and Communications Agency Traficom, 27th of September 2024

Publication series and number
Traficom Research Reports 04/2024
ISSN (e-publication) 2669-8781
ISBN (e-publication) 978-952-311-952-9

Keywords
State-of-art cyber and information security solutions, adoption of technologies, small and medium size enterprises, financial support, national cyber security capacity

Abstract
The evaluation assessed the direct and indirect impacts of Finnish Transport and Communications Agency's National Cyber Security Centre's National Coordination Centre's (NCC-FI) financial support for SMEs to implement state-of-art information and cyber security solutions and innovations. The main methods and data sources of the evaluation were analysis of project plans, applications and data, beneficiaries survey, expert interviews, literature review and validation workshop.
In terms of direct impacts to beneficiaries, the evaluation found that the financial support has well fulfilled its purpose and its direct impact to beneficiaries can be considered high. Almost all the projects (95 %) stated that they have successfully implemented their technology upgrading and reached the project goals. The companies were also reporting increased resilience against cyber-attacks. In terms of indirect impacts, the evaluation was looking at effects on cyber security market and overall national cyber security capacity. The financial support has generated some additional demand for the provision of IT services with the volume of around EUR 0.9 million. The services were mainly provided by Finnish companies. The purchased technological solutions were mainly those provided by international large-scale companies. In terms of proportionality and appropriateness, it seems clear that the volume (2 MEUR) is limited, when considering the national needs. Therefore, volume is appropriate either as a targeted support and incentive to address certain identified challenges. The grant size (max EUR 60 thousand) could be equally effective in a slightly smaller form (e.g. EUR 20 thousand), thus allowing for more grants to be delivered.
The evaluation recommends that further support for companies to upgrade their cyber security should be ensured, the effectiveness could be increased by decreasing the size of individual grants, while expanding the number of given grants, the instrument should support holistic approach to cyber security and encourage companies to take actions beyond adoption of technology and that financial support should be complemented with non-financial support, such as technical guidance and sharing of good (process) practices, to enhance its effectiveness.

Contact-person
Annalotta Saarikoski

Language
English

Confidence status
Public

Pages, total
57

Distributed by
Finnish Transport and Communications Agency Traficom

Published by
Finnish Transport and Communications Agency Traficom

Table of Contents

1 Introduction

1.1 Background and objectives of the evaluation

During the years 2023-2024, the Finnish Transport and Communication Agency (Traficom) and its National Cyber Security Centre (NCSC-FI) has granted a total of six million euros of financial support in information security development (the so-called information security voucher) to improve companies' own information security. In addition to this, as a part of Traficom and NCSC-FI, the National Coordination Centre Finland (NCC-FI) has received financial support from the Digital Europe Programme, part of which NCC-FI has distributed to third parties during 2023–2024. The financial support has been primarily aimed at strengthening the capabilities of small and medium-sized enterprises as well as enhancing Finland's national capacity and infrastructure to defend against cyberattacks.

The NCSC-FI has commissioned two impact evaluations, one of which focuses on the support for the development of information security and the other on the support on implementation of state-of-the-art cyber and information security solutions and innovations. This report provides the outcomes of the latter impact evaluation.

The evaluation questions are divided into the following three groups.

1) Direct and short-term impact on beneficiaries:

- How has the financial support affected the recipients' own cyber and information security?
- To what extent has the financial support encouraged beneficiaries to implement measures that improve their own information security (incentive effect)? To what extent would these measures have been left unimplemented without the financial support?
- To what extent has the financial support met the needs of the recipient companies?
- To what extent has the financial support affected the beneficiaries to competitiveness/competitive situation (competitive effects)?
- To what extent has the financial support had the expected effects?
- How has the financial support affected the different recipients of the support, the company's size, location and activities by industry?

2) Short and long-term indirect impact:

- How has the financial support affected Finnish cyber security companies and to their business?
- How has the financial support affected other companies?
- How has the financial support affected society's cyber security capacity?
- How has the financial support affected Finland and the European Union strategic autonomy on cyber security and competitiveness?

3) Proportionality and appropriateness:

- To what extent has the financial support been proportionate to the problems to be solved?
- To what extent could the same effect have been achieved with less financial support or with a different form of support?
- To what extent could the same effect have been achieved with other measures?
- To what extent was the chosen financial support instrument the most effective, and could alternative instruments have been more suitable or effective?

1.2 Evaluation methods and information sources

1.2.1 Evaluation framework

The general framework for impact evaluation is based on the Theory of Change model (see Figure 1) and its associated general impact evaluation criteria: relevance, coherence, effectiveness and impact:

Relevance: Alignment of the project's objectives with the targeted challenges; identification of potential gaps.

Coherence: **Internal Coherence**: The overall framework formed by the project's activities, how they are coordinated, how they align, and the synergies between them. **External Coherence**: The project's compatibility with other national strategies, projects, and programs addressing the same societal challenge.

Efficiency: The operating model of the projects and the project framework as a whole, including the organization and implementation of the overall project and key initiatives.

Effectiveness: The project's ability to achieve its concrete (short-term) objectives.

Impact: The project's ability to achieve its long-term goals, as well as opportunities to enhance its impact and prerequisites for doing so.

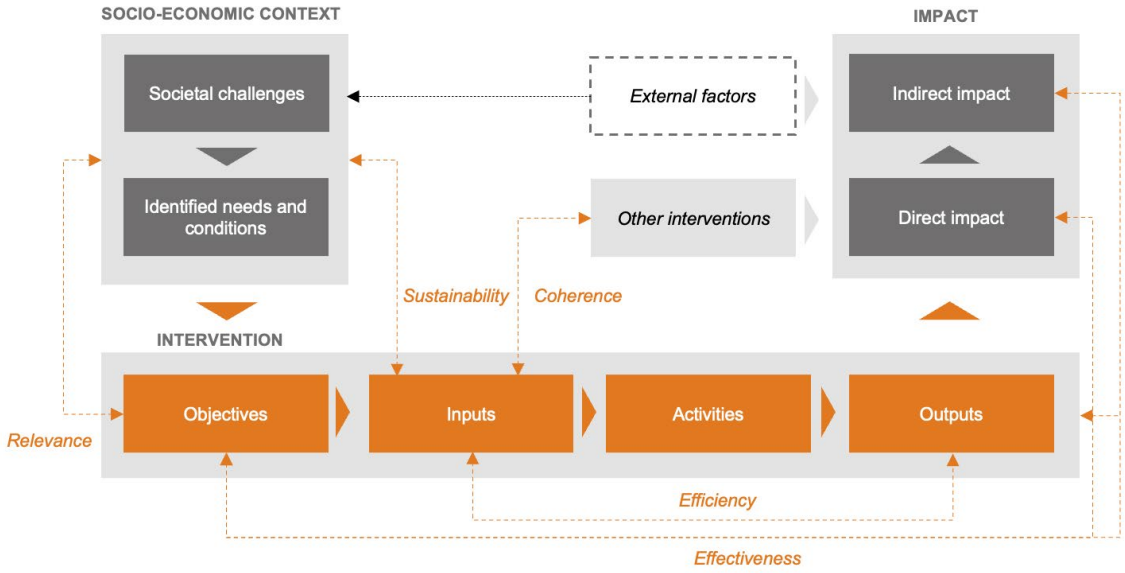

Figure 1. Analytical framework for the impact evaluation (Theory-of-Change). Source: 4FRONT, adapted from OECD (2021) Applying Evaluation Criteria Thoughtfully. OECD and European Commission Better Regulation Toolbox, Tool #46 Designing the Evaluation.

The framework was further developed to model programme specific impact pathways (see page Figure 3, page 16) of the financial support. This programme specific impact framework was used to guidance the data collection and the analysis conducted on the data.

1.2.2 Methods and data sources

The evaluation employed a comprehensive methodology combining multiple approaches to assess the impacts of the financial support programme. Document analysis of project plans, final reports, and other documentation formed the basis for drafting survey questions and understanding the project's structure. Expert interviews and a literature review provided in-depth insights into the operating environment and the specific needs of SMEs. Funding data was analysed to evaluate the allocation and distribution of resources. A beneficiaries' survey, complemented by Eurostat data, was conducted to assess the direct impacts of the financial support programme and to compare the baseline security levels of beneficiaries and other companies in Finland. Finally, a workshop with NCSC-FI staff and external experts was organised to validate and refine the evaluation findings, ensuring their relevance and coherence.

Table 2. Methods and data sources

Method	Description
Document analysis	Project plans, final reports, and other documentation were analysed in the evaluation. Reports were used to draft the survey questions.
Literature review	A literature review was conducted to get an in-depth understanding of the operating environment and the needs of SMEs.
Expert interviews	Expert interviews were used to deepen the understanding of the operating environment and the needs of SMEs. A total of 7 external experts were interviewed and a total of 5 experts from NCC-FI.
Data analysis	Financial support data was analysed to get an understanding of the distribution of the financial support.
Beneficiaries survey	A survey was sent to beneficiaries of the financial support programme to assess the direct impacts. The survey was also quantifying the findings of the project reports. Additionally, Eurostat data was used to compare the baseline security level of beneficiaries and companies in Finland. The survey was sent to all 50 beneficiaries and got a total of 44 responses.
Workshop	The evaluation organised a workshop for NCSC-FI staff and external experts to validate and further develop the findings of the evaluation.

The evaluation was looking at both direct and indirect impacts of the financial support. Direct impacts are related to the beneficiaries and their security levels. Indirect impacts are related to other companies, cyber security market and overall security capacity in Finland and EU.

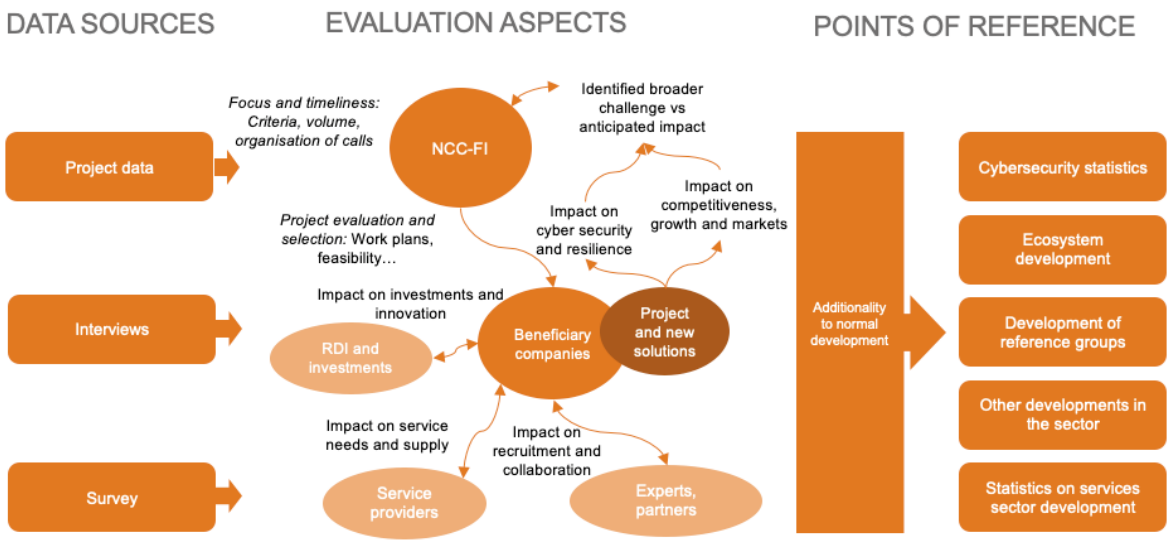

Figure 3. Illustration of the evaluation setup with key data sources and reference points.

Limitations

The findings of the evaluation are based on self-assessment of the beneficiaries, views of experts and in-depth analysis of the operating environment and its needs. The analysis can provide a good estimate of the direction of the impacts (positive/negative). However, with the available data

sources, it is impossible to quantify the size of the effect or conduct an empiric counterfactual analysis to determine an actual causal effect. Moreover, many of the long-term impacts take time to realise. Therefore, the evaluation was identifying anticipated and reported impacts.

2 Description of the financial support

2.1 Background and context

The European Cybersecurity Competence Centre (ECCC), together with the Network of National Coordination Centres (NCCs), is Europe's framework to support innovation and industrial policy in cyber security.[1] This ecosystem is to strengthen the capacities of the Cybersecurity Competence Community, shield economy and society from cyberattacks, maintain research excellence and reinforce the competitiveness of EU industry in this field. ECCC and the Network of NCCs together aim to enhance Union's leadership and strategic autonomy in the area of cyber security through joint investment in strategic cyber security projects.

In the background of the establishment of ECCC and NCCs is the EU Cybersecurity Strategy 2020 (previous 2013), which defines the general principles, directions and goals of the development (European Commission 2020). The strategy particularly highlights the EU's collective awareness and lack of preparedness for threats. As one answer, it proposes the establishment of a European centre of expertise and its Network of National Coordination Centres.

The *EU Directive 2016/1148 on the Security of Network and Information Systems* (European Parliament 2016), which has since been replaced by the *EU Cybersecurity Directive 2022/2555 the so-called NIS2 Directive* (European Parliament 2022*)*, and especially *EU Regulation 2021/887 of the European Cyber Security Industry, Technology and Research Competence Centre* (European Parliament 2021) have been central to the implementation of these strategies and the establishment of a Network of National Coordination Centres. This is also where the need for improving the resilience and the technological and industrial capabilities has been raised, along with the use of high safety standards and comprehensive solutions. The regulation also defines the tasks, cooperation, etc. of the National Coordination Centres.

The national implementation of the EU regulation was done in Finland with the amendment of the *Act on the Transport and Communications Agency*

[1] For more information on ECCC and NCCs, see: https://cybersecurity-centre.europa.eu/index_en

935/2018 (Valtioneuvosto 2018) by expanding the tasks of the National Cyber Security Centre Finland (NCSC-FI). The tasks of the National Coordination Centre Finland (NCC-FI) are laid down in the EU regulation (2021/887) and one of those tasks is the provision of financial support to third parties.

The justifications for the act also state that appropriate handling of the obligations requires cooperation between different national actors (Business Finland, VTT Technical Research Centre of Finland Ltd., Finnish Information Security Cluster, National Emergency Supply Agency, Digital and Population Data Services Agency, universities and colleges). In this way, the competence found in Finland would be harnessed in the most expedient and efficient way possible to support the creation of new companies, and for the benefit of the entire cyber security community.

According to the law, the *Finnish Cybersecurity Strategy 2019* (Valtioneuvosto 2019) should be taken into account in the orientation and emphasis of the activities. The strategy has been updated by the current government into the *Finnish Cybersecurity Strategy 2024-2035* (Valtioneuvosto 2024*)*. The strategy sets the most important goals for the development of the cyber operations environment and also takes into account e.g. the requirements of the NIS2 cyber security directive.

To support the implementation of the 2019 strategy, a national *Cyber Security Development Programme* (Liikenne- ja viestintäministeriö 2019) was drawn up under the leadership of the Ministry of Transport and Communications. The primary goal of the programme was to build a cyber security ecosystem in Finland. In the core of the long-term development were improving of cyber security skills, supporting the domestic cyber security industry and intensifying cooperation between the public administration and the business world. In the current national cyber security strategy (2024-2035), key measures are aimed at four directions: *1) competence, technology and RDI, 2) preparedness, 3) cooperation* and *4) reaction and countermeasures*. The financial support that is now being evaluated is especially relevant in terms of the first main direction of the new strategy.

2.2 Objectives of the National Coordination Centre Finland

The National Coordination Centre Finland (NCC-FI) officially started its operations at the beginning of 2023. The task of the NCC-FI is to create conditions for the Finnish cyber security ecosystem, such as companies, universities and research institutes, to participate in international research and development activities and receive funding from EU funding programs. In doing so, NCC-FI assembles and develops a national competence community. The purpose of the community is to bring together key actors from the

public and private sectors and to develop joint work between actors to enable and improve cyber security research, development and innovation.

In particular, NCC-FI supports 1) the participation of Finnish actors in cross-border EU projects and promotes obtaining EU funding in line with national priorities. 2) The central task of the NCC-FI is to distribute financial support to Finnish operators for activities that improve cyber security. The first national call round for financial support was opened in June 2023.

According to the national strategy of the NCC-FI, the financial support is to be directed especially to the promotion of research and development in SMEs, as well as to the introduction of new cyber security solutions and the sharing of information about state-of-the-art solutions. The scope of the financial support call rounds can vary and is announced in connection with each call round.

As a national coordination centre, the NCC-FI does not directly distribute EU funding from the EU funding programmes, but when carrying out special activities of the European Cybersecurity Competence Centre (ECCC), it can grant financial support to third parties as part of its own projects. In accordance with the conditions defined in the grant agreement of NCC-FI's EU project in 2023-2024, financial support to third parties was limited up to a EUR 60 thousand per project. To this end, the NCC-FI received total of EUR 1 million (50 % of the total budget) from EU funding from the *Digital Europe Programme*[2] to support the implementation of cyber security solutions, especially by the SMEs in 2023 and 2024. The EU funding requires a corresponding amount of national funding, too.

The overall objective of NCC-FI's Digital Europe project[3] is to strengthen the centre's prerequisites for performing its tasks as a National Coordination Centre in accordance with the EU regulation. The project has a duration of two years (1/2023-12/2024) and has five sub-objectives: 1) support the ECCC, 2) foster the Cybersecurity Competence Community in Finland, 3) support cyber security capacity building in Finland, 4) foster cross-border cooperation and preparation of joint actions and 5) promote the dissemination and communication of relevant outcomes of the project. The financial support for third parties examined in this evaluation belongs to the national cyber security capacity building sub-objective (3).

In the project plan, it has been stated that the financial support is needed to build national capacity in cyber security with speed and impact. Financial support to third parties is aimed particularly at strengthening the uptake

[2] The Digital Europe Programme. https://commission.europa.eu/funding-tenders/find-funding/eu-funding-programmes/digital-europe-programme_en
[3] Project (101100631) "Building Capacity for the Finland National Coordination Centre for Cybersecurity in Industry, Technology and Research"

and dissemination of state-of-the-art cyber security solutions especially by SMEs. Financial support is to be granted to companies through an open public call round and in two different calls rounds. The maximum amount of financial support per project is EUR 60 thousand and the companies' co-funding requested from the recipients is 0-50%. In the project plan, it is anticipated that in total 32 projects will be supported in 2023-2024. All of the applications go through an evaluation process and the best applications receive funding within the call budget. The applications were first evaluated against the eligibility criteria and the terms and conditions of the financial support. Applications that met the eligibility criteria proceeded to the evaluation stage. In the evaluation stage, the proposals were scored according to relevance, implementation, and impact of the project as presented in the call for proposals document.

2.3 Financial support for implementation of state-of-the-art cyber and information security solutions and innovations

The financial support primarily aims to strengthen the applicant companies' own capabilities as well as Finland's national capacity and infrastructure to defend against cyber security threats. Financial support is granted for projects that achieve long-term impacts in improving cyber security within the applicant company.

Financial support is not granted for the development or innovation of new products or services if such development or innovation does not directly enhance the applicant company's own cyber security.

A state-of-the-art solution or innovation to be implemented represents relatively new and advanced technology. State-of-the-art solutions utilize, for example: advanced automation, machine learning, artificial intelligence, quantum-resistant encryption solutions, or new network technologies (such as SDN, SD-WAN, or 5G). Solutions that have been in use for a long time, such as traditional firewalls, antivirus software, or virtual private networks, are not considered as state-of-the-art solutions. However, traditional solutions can be considered as state-of-the-art if their implementation follows a new and advanced approach.

Eligible Costs include salaries, purchased services, other purchases (e.g., equipment, infrastructure, or other fixed assets), rental and licensing costs (e.g., equipment and software), internal communication costs, reasonable travel costs, costs related to final project reporting and indirect cost flat-rate.

Table 4. Basic information on the financial support

	Financial support by the National Coordination Centre
Objective	Support the adoption of state-of-the-art cyber security and information security solutions and innovations by companies.
Focus group	Micro and small- to medium-sized enterprises (SMEs) registered in Finland.
Financial support type	Grant type: De minimis aid. Maximum grant per applicant/project: EUR 60 thousand. Co-financing requirement: Minimum of 25%.
Time period	First call round open: 16.6.-18.6.2023, project implementation time: 16.5.2023-31.5.2024 Second call round open: 2.1.-1.3.2024, project implementation time: 2.1.-30.9.2024
Volume	Total financial support pool: EUR 2 million. Project support ranges from EUR 6,622 to EUR 60 thousand.
Beneficiaries	50 SMEs supported (2023 13/17 applications; 2024 37/170 applications).
Selection process	Applications that meet the eligibility criteria are scored according to relevance, implementation, and impact of the project as presented in the call for proposals document.
Monitoring and evaluation	A report on the use and impact of the support is required after project completion.

3 Evaluation findings

This chapter presents the findings of the evaluation. The findings are divided into two sections, one looking at the direct impacts on the beneficiaries and the other one indirect impacts. The impact assessment is following the impact model (Figure 2) developed for the financial support which is an elaboration of the Theory of Change framework (Figure 1).

The evaluation findings are organized as follows: first section looks at the distribution of financial support, the second section looks at the direct impacts on the beneficiaries and the third section looks at the indirect impacts on the cyber security market and overall national cyber security capacity.

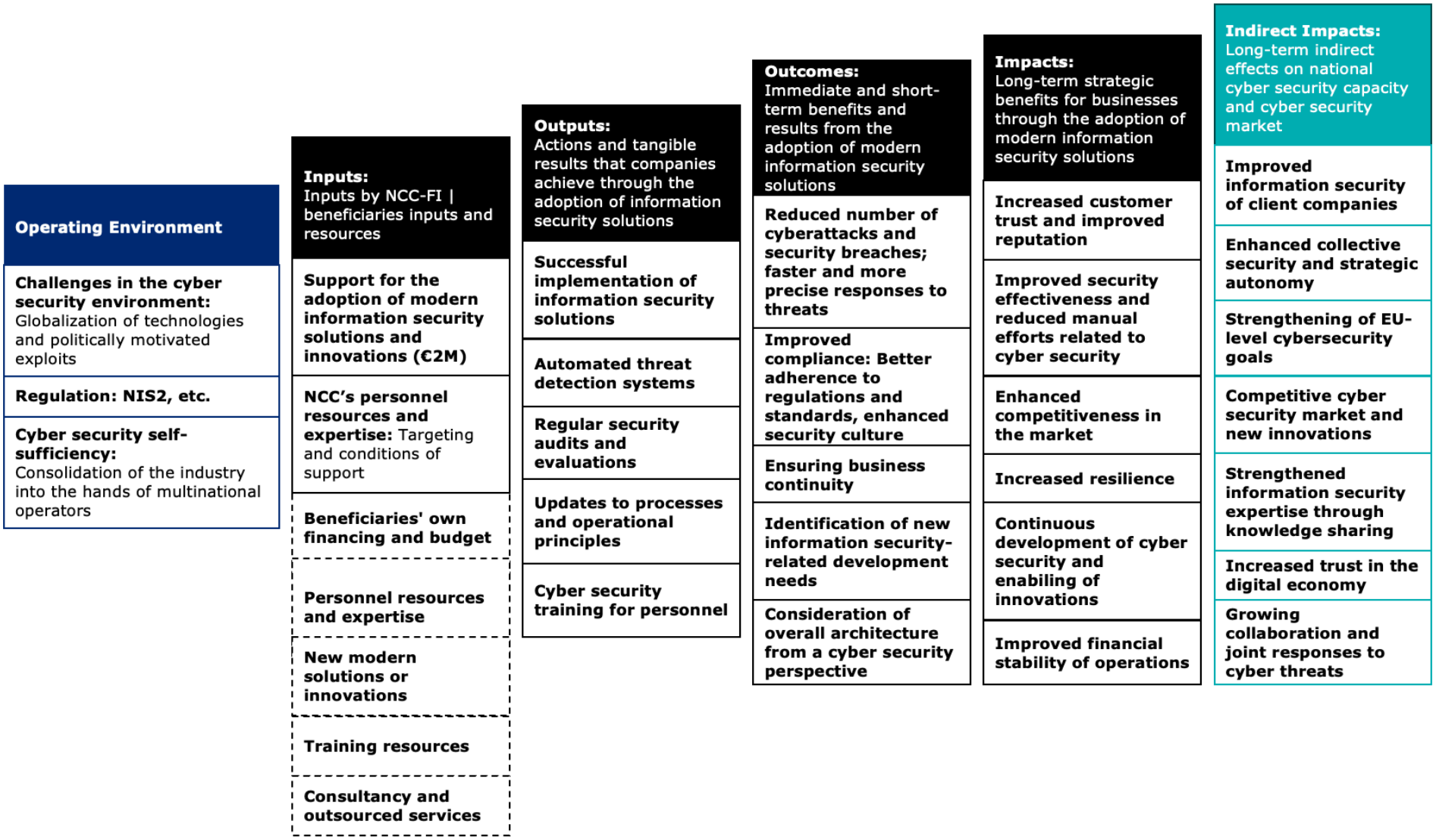

Figure 3. Elaborated analytical framework for this impact assessment. Source: 4FRONT Oy.

3.1 Distribution of financial support

NCC-FI as a part of NCSC-FI and Traficom granted financial support for SMEs to deploy state-of-the-art cyber security and information security solutions and innovations during 2023–2024 with total of EUR 2 million. The financial support was granted to a total of 50 projects. Approximately EUR 1 million was granted to small companies (<50 personnel), EUR 500 thousand to medium sized companies (<250 personnel) and EUR 500 thousand to micro companies (<10 personnel). Average project size was around EUR 40 thousand.

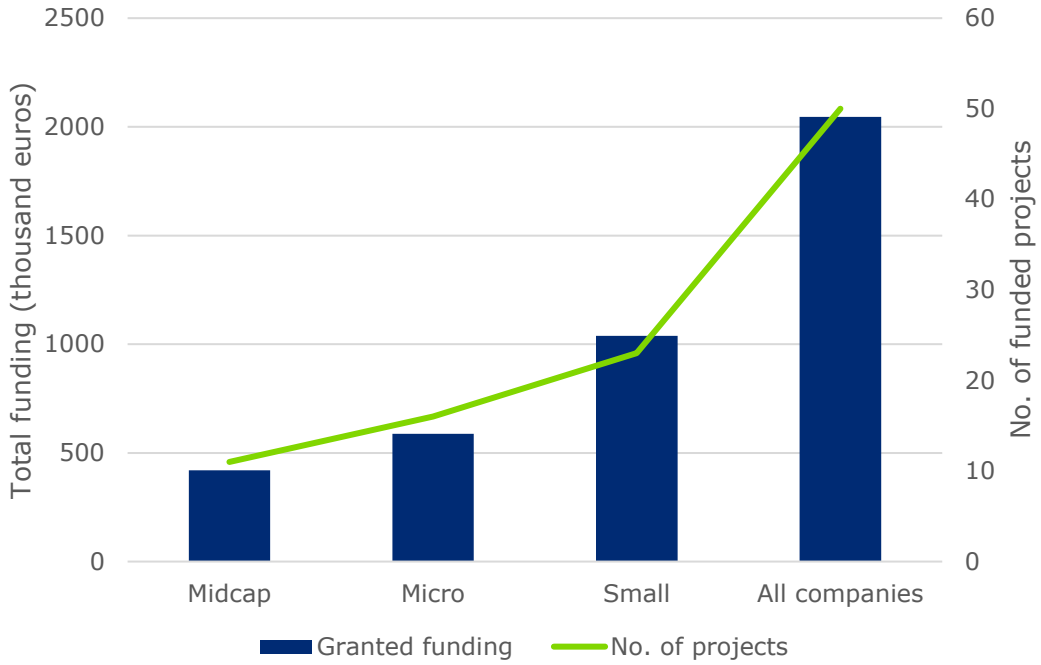

Figure 4. Total financial support and number of supported projects per size of the company. Source: NCC-FI

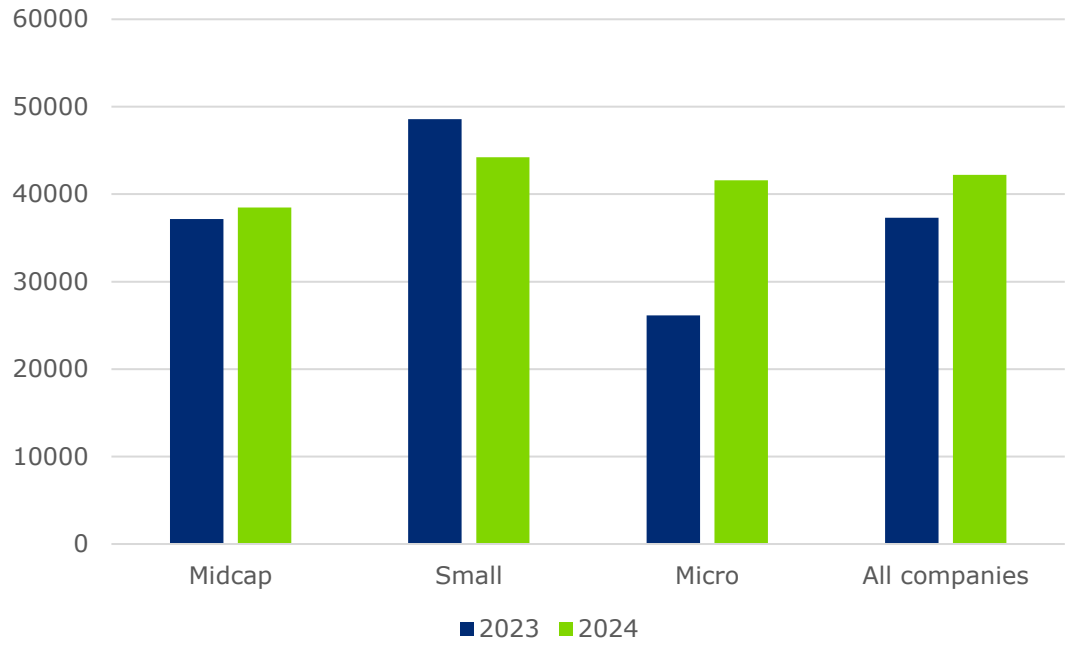

Figure 5. Average project size per size of company. Source: NCC-FI

The financial support has been very popular. The programme received a total of 187 applications out of which 50 were granted financial support. In terms of applied financial support, the programme received applications worth of nearly EUR 7 million, which means that the programme could grant only 30 % of what was applied for. The number of applications increased significantly during the second call round in 2024. This is largely explained by increased communication from NCC-FI, as explained by the staff. Another factor may be related to naming of the financial support. First round was called "financial support for deployment of state-of-the-art cyber security solutions and innovations" and the second round "financial support for deployment of state-of-the-art information security solutions and innovations". It was explained by the NCC-FI staff that they made a strategic decision to rename the call in order to make it more approachable to all kinds of companies regardless of their maturity on cyber security knowledge.

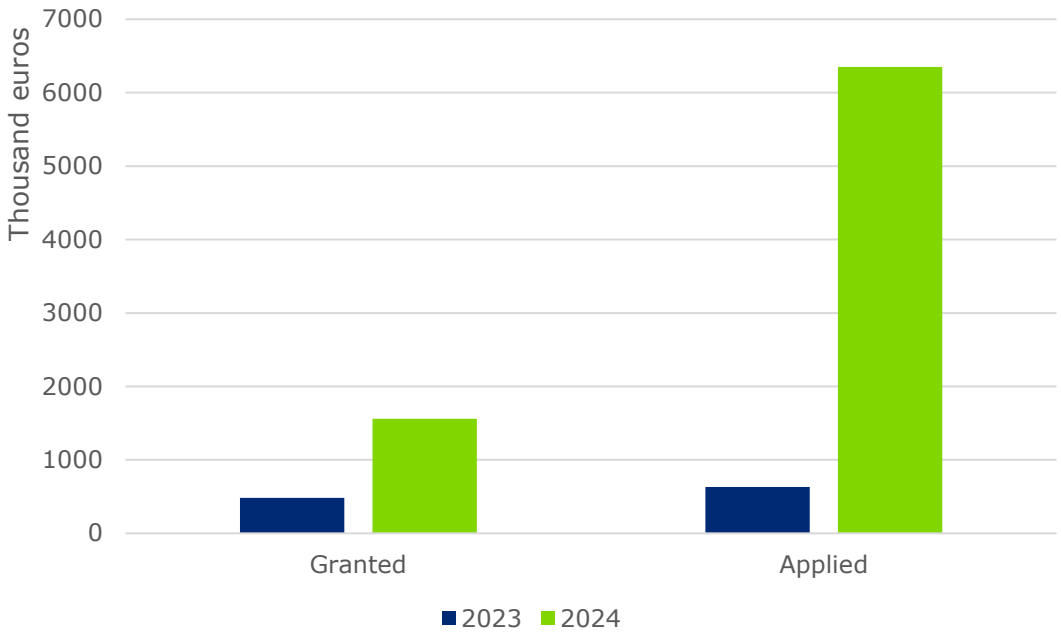

Figure 6. Granted and applied financial support. Source: NCC-FI

There was a large regional variation on how grants were awarded, which is in line with how companies are located in Finland. 50 % of the financial support was granted to Uusimaa region and 12 % to Pohjois-Pohjanmaa. Rest of the regions received total of 38 % of financial support. Uusimaa, Pirkanmaa and Pohjois-Pohjanmaa applied the most financial support.

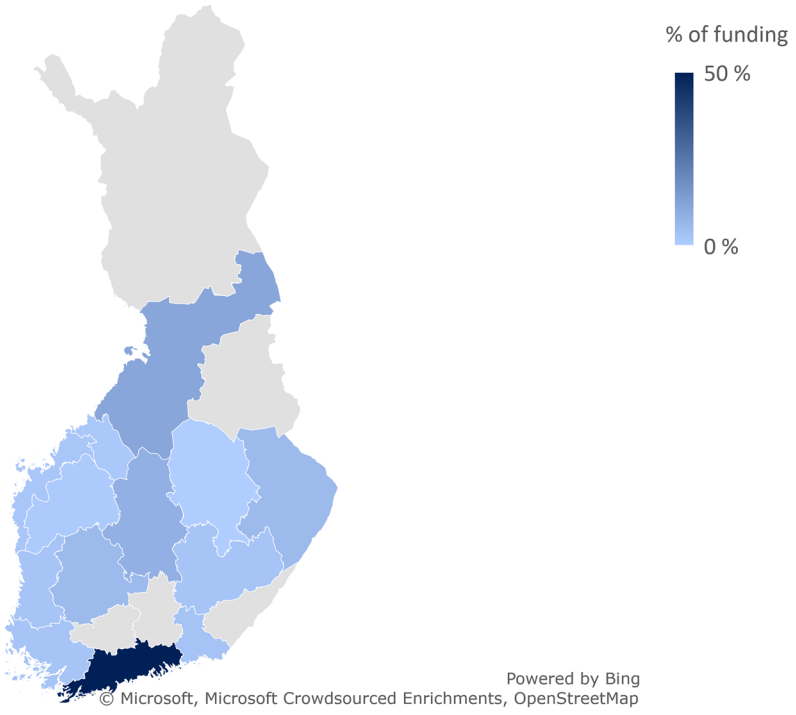

Figure 1. Share of granted financial support per region. Source: NCC-FI

Majority of the financial support was granted to companies operating in the sector of information and communications (ICT) (EUR 1 million). The second largest sector was Professional, scientific and technical activities (PST) (EUR 0.26 million) and manufacturing (EUR 0.61 million). Within ICT sector, the most common subsector was software design and development and in terms of PST, the most common subsector were management consulting, mechanical and process engineering and patent offices.

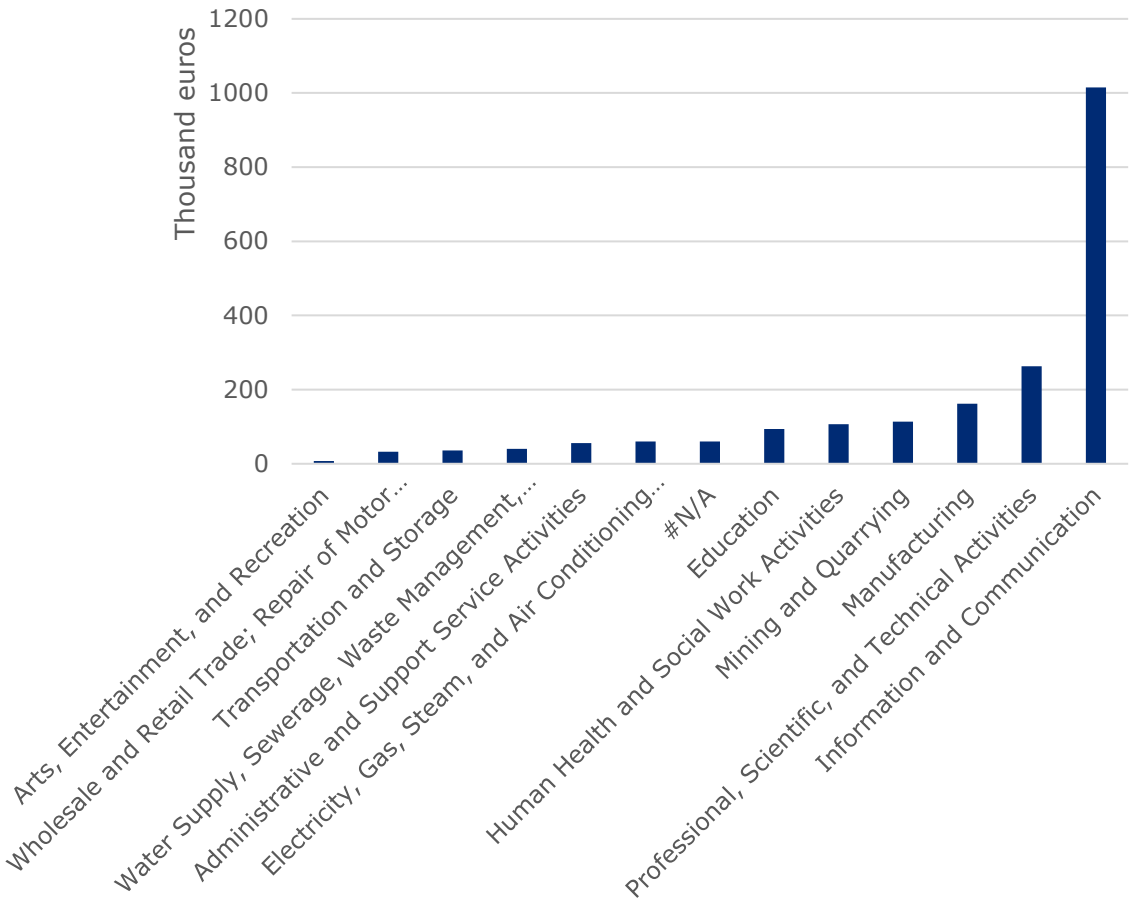

Figure 2. Granted financial support per sector (NACE 2). Source: NCC-FI

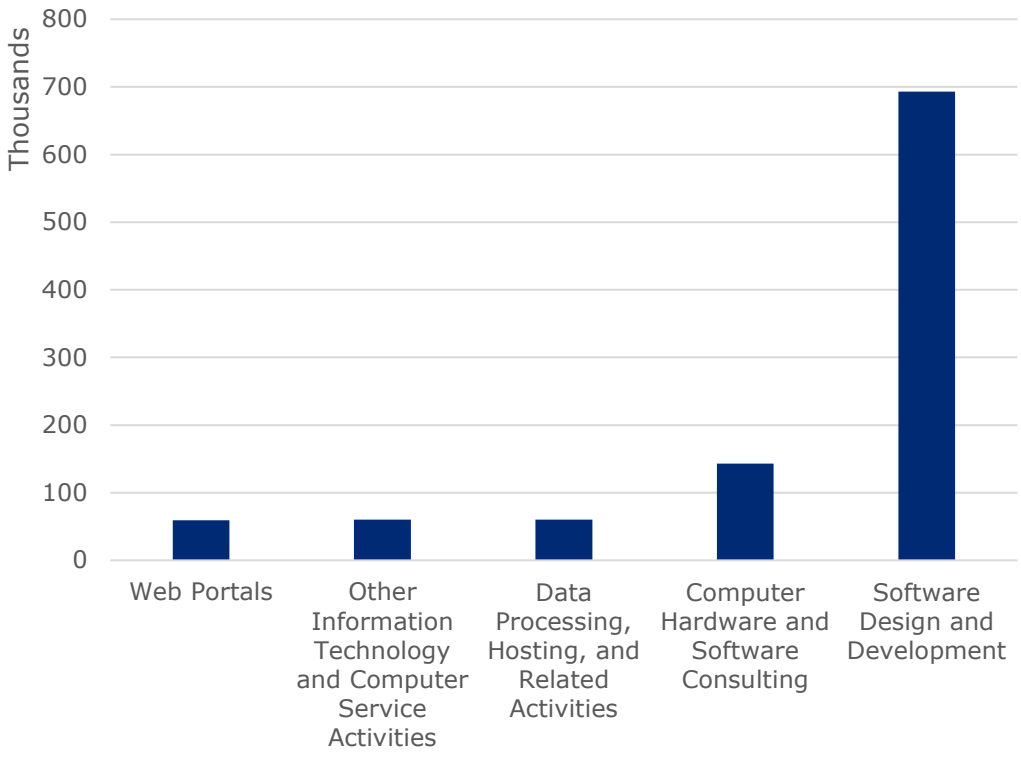

Figure 3. Granted financial support per subsector in information and communications. Source: NCC-FI

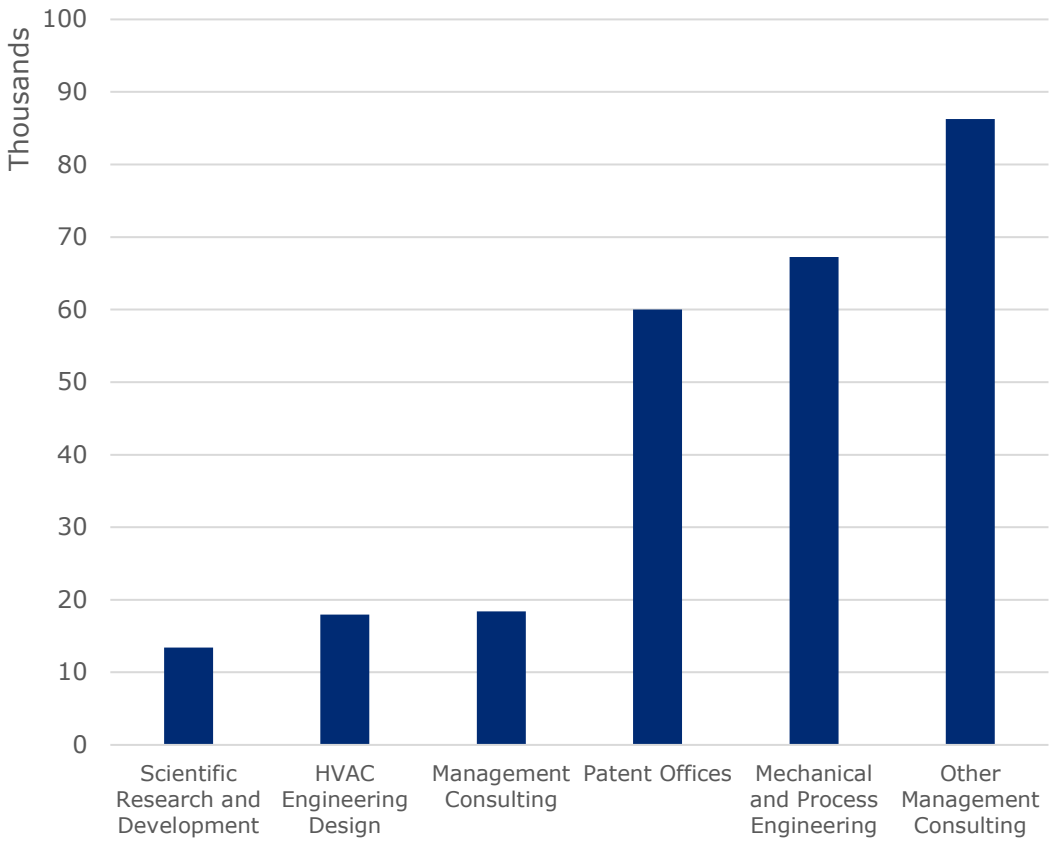

Figure 4. Granted financial support per subsector in Professional, Scientific, and Technical Activities. Source: NCC-FI

3.2 Direct impact on beneficiaries of the financial support

3.2.1 Activities and inputs

The main aim for the financial support is to support micro, small and medium-sized enterprises to uptake state-of-the-art cyber and information security solutions and innovations and improve their capacity. SMEs have typically limited resources, and they rarely have staff specialised in cyber and information security issues. A typical supported project allocated part of its financial support into purchasing services from specialised companies to assist in integration of the solution/innovation into their IT system. Most of the service providers were Finnish. The purchased solutions/innovations were typically provided by large multinational companies such as Microsoft, and they were often selected based on their suitability to their existing IT system, e.g., Microsoft Teams → Microsoft cyber security services. Other inputs from the beneficiaries' side included allocated workhours on the project.

Based on the survey findings, approximately 55 % of the supported companies used the grant to update and further develop their existing technologies. The level of external support varied across the beneficiaries. Nearly half of the companies implemented the project by mainly using internal staff and for the other half, the project was implemented mainly by using external support (e.g., consultants or IT services). Most of the projects were using ready-made technologies, however, a bit over 20 % mentioned that they developed technology themselves and 15 % said that they purchased the development via external service provider.

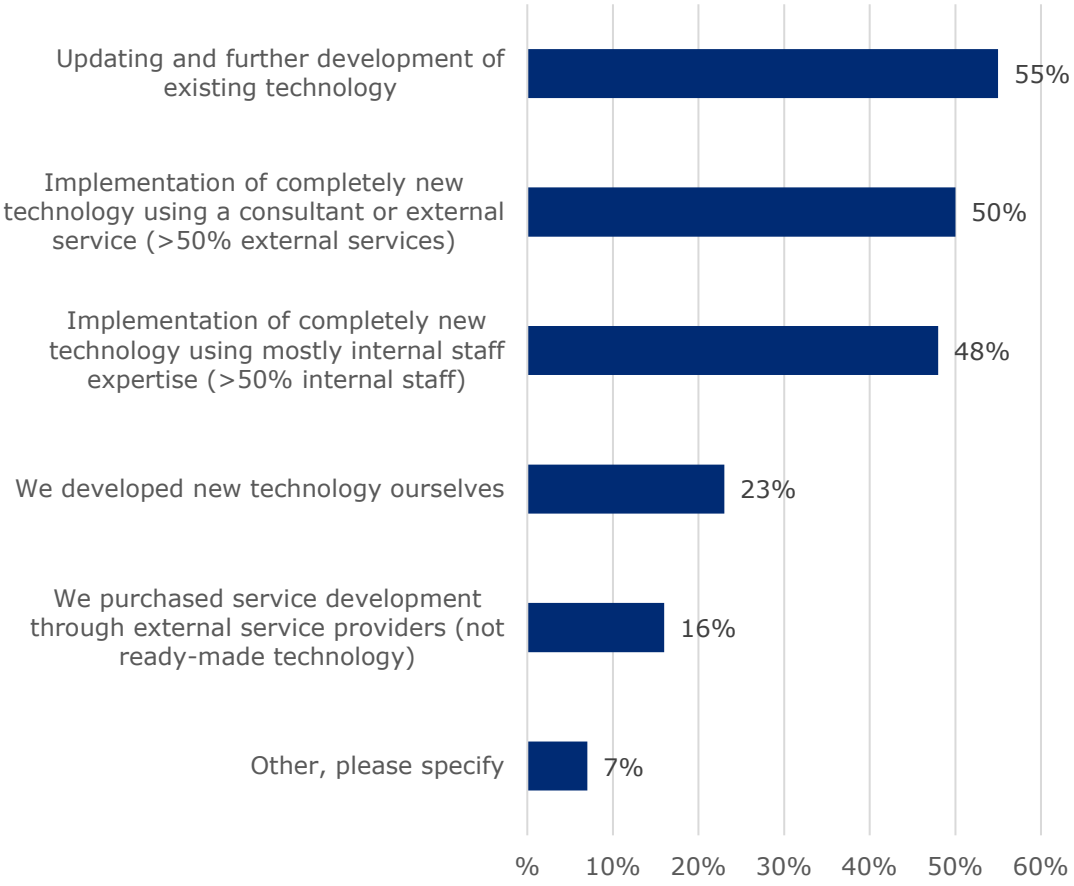

Figure 5. Question: How was the project implemented? (you can select multiple options). *n=44 (N=50).*

The projects were targeted to improve a large variety of cyber and information security issues. Most commonly, the targets involved information security (e.g., customer data, such as health data, trade secrets, financial transactions, critical infrastructure, other sensitive personal data), network security and administrative security. 55 % also said that the project will improve the security of their devices and operational technology.

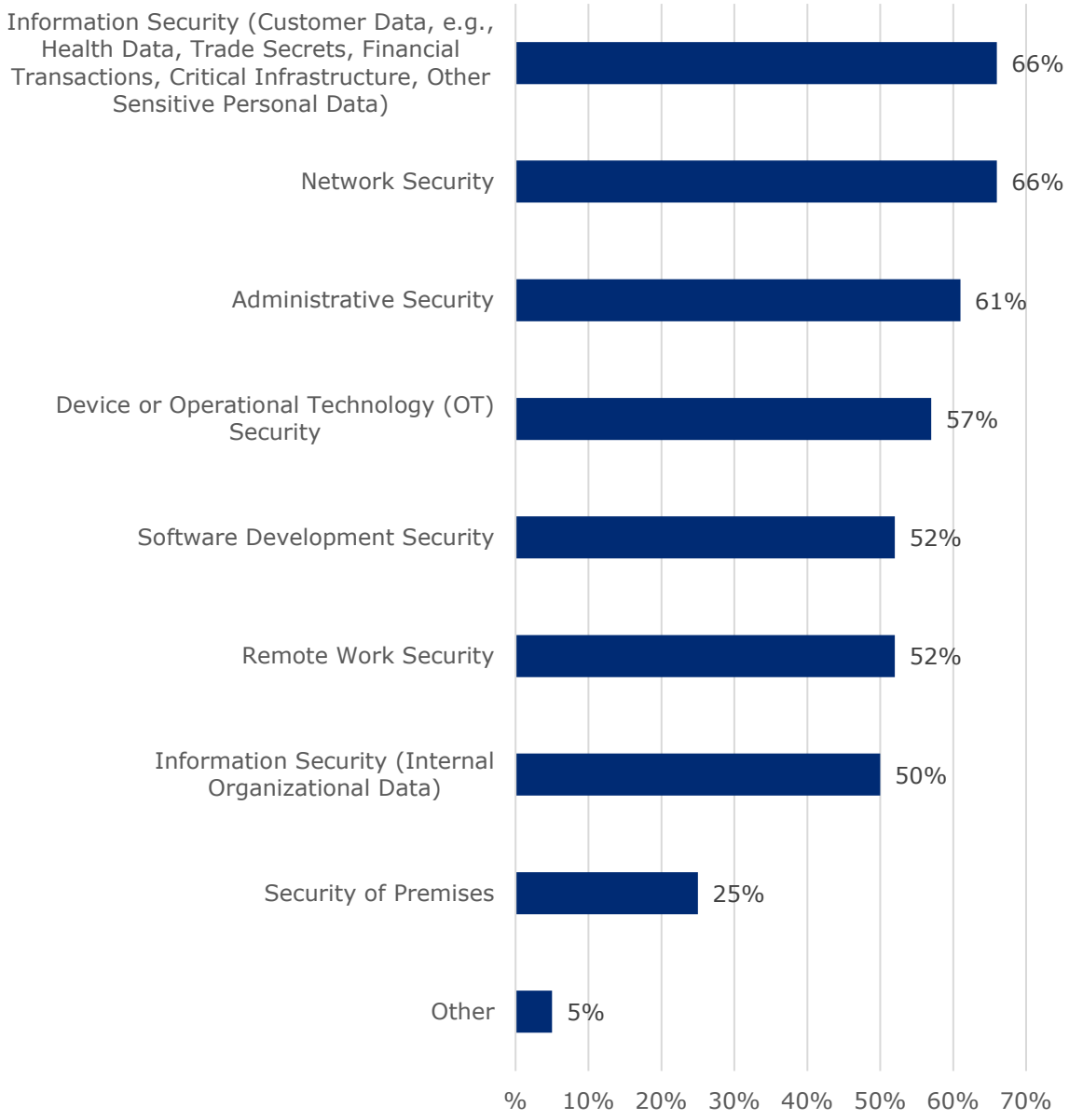

Figure 6. Question: "What types of activities does the improved information/cyber security implemented in the project target (directly or indirectly through customers)?" *n=44 (N=50).*

3.2.2 Additionality of the financial support

An important rationale for financial support for third parties is that it ignites something that would not happen without it. This may involve e.g., time and scale. In other words, the support should make a larger positive change, than what would have happened without the financial support or it should speed up the process.

According to the beneficiaries' survey, the financial support was critical for the implementation of measures. 93 % stated that the measures would not

have been implemented at all or only partially without the support. The support also significantly accelerated the implementation of the measures (73%). 27 % reported that the financial support accelerated the uptake of technologies to some extent.

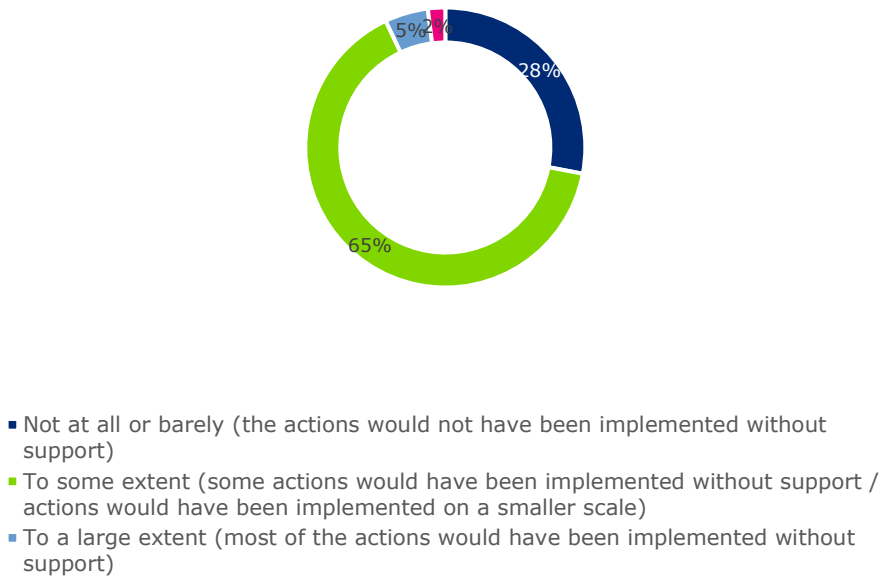

Figure 7. Question: To what extent would the actions implemented in the project have been carried out without support? *n=44 (N=50)*

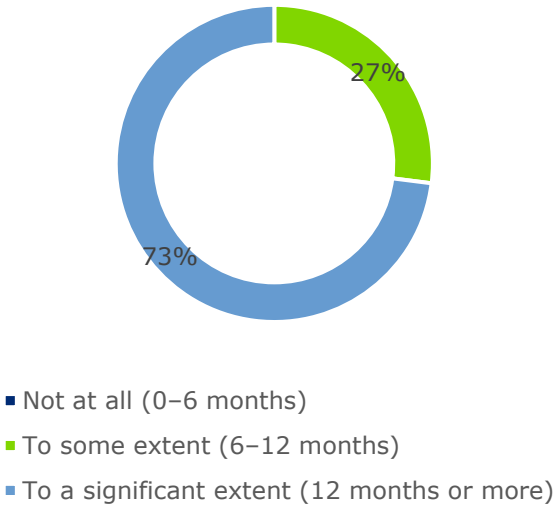

Figure 8. Question: Evaluate to what extent the support accelerated the implementation of the actions carried out in the project in terms of time? *n=44 (N=50)*

3.2.3 Cyber security impact

The direct reported impacts to the beneficiaries were evaluated using an impact framework that classifies results into direct outputs, short-term outcomes and anticipated long-term impacts (see figure 2). Overall, the results of the survey show that the beneficiaries are perceiving the outcomes of the financial support as very positive.

Overall, the survey companies reported that the project goals were achieved very well (61 %) or fairly well (38 %).

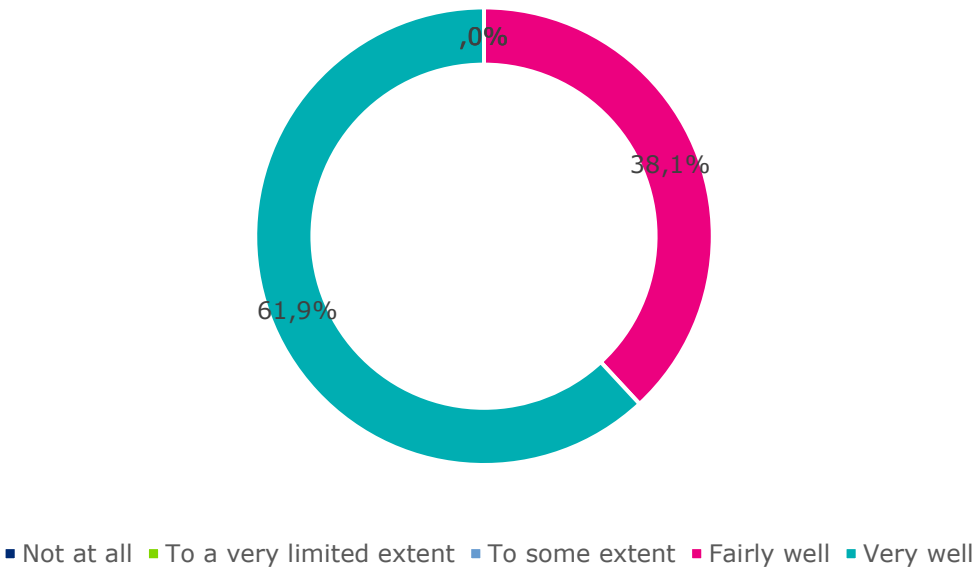

Figure 9. Question: To what extent were the project goals achieved? *n=44 (N=50)*

The projects were reportedly very successful in terms of their main goal. Altogether 95 % of the respondents state that they successfully implemented and up took the technology they were planning to. In addition to up taking solutions and new technologies, many of the companies reported to have taken other actions to integrate cyber and information security holistically. 77 % of the respondents said that during the project, they implemented automated systems to detect threats. 65 % said they also updated their processes and operating principles regarding security and nearly 60 % said they organised cyber/information security training for their staff. While the results regarding activities seem holistic and thorough, only 40 % stated that they organised information security audits and assessments during the project. As emphasised by the interviewed external experts, it is crucial to uptake such technologies that best improve the specific risks that the company has. It is however possible that the companies may have organised information security audits before applying the financial support.

While updating processes, training staff and other supporting activities were not targeted actions in the financial support call rounds, they were still eligibles costs. According to the call for proposals documents, the financial support was mainly targeted for the implementation of solutions and innovations.

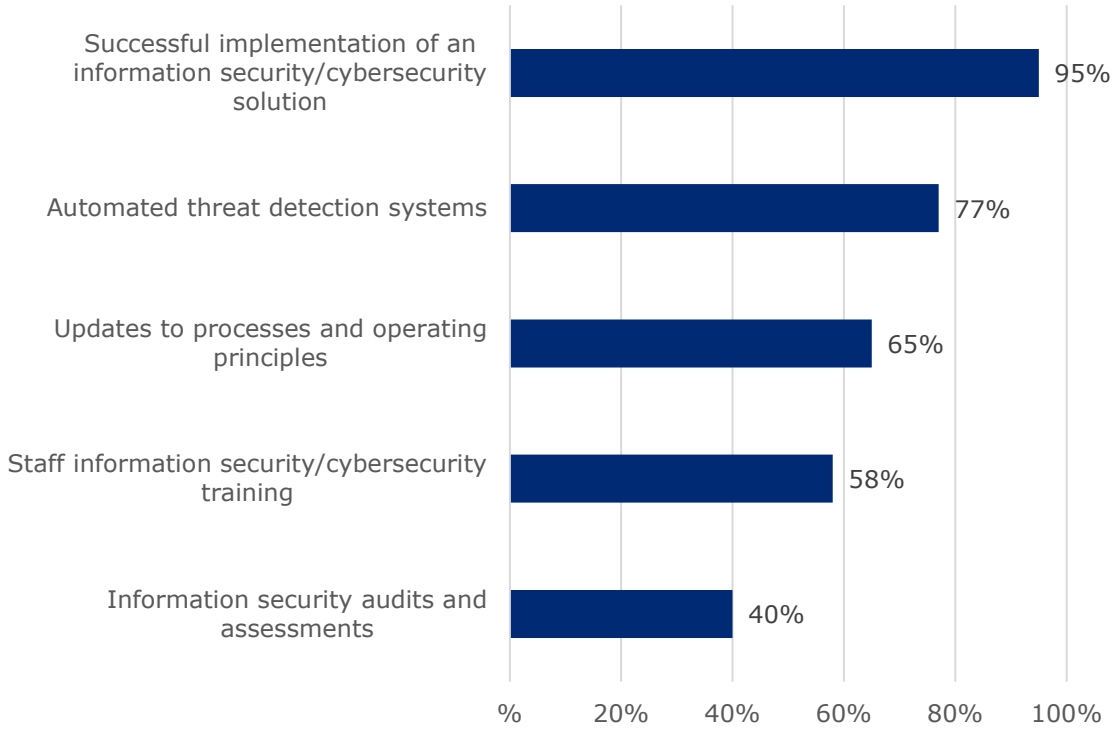

Figure 10. Question: What kinds of outcomes have been achieved in your company with the help of financial support? (You can choose multiple options) *n=44 (N=50)*

In terms of short-term results, approximately 80 % companies are self-assessing that the project improved their ability to respond to threats, enhanced information security awareness across the organisation and allowed them to implement their security via overall architecture instead of isolated security solutions. By integrating cyber security into the overall architecture, companies create a unified, efficient, and resilient environment that not only protects assets but also supports strategic growth and compliance needs as well as support positive security spillover effects for their networks, such as clients and supply chains. 82 % reported that the project helped to identify new security related development needs, which is a good predictor of financial support's long-term impact, and a mindset change within the beneficiaries. Approximately 60 % mentioned also, that they are better equipped to comply with regulations and standards (such as NIS2 and GDPR). Half of the companies reported that they have managed to reduce number of cyber security attacks.

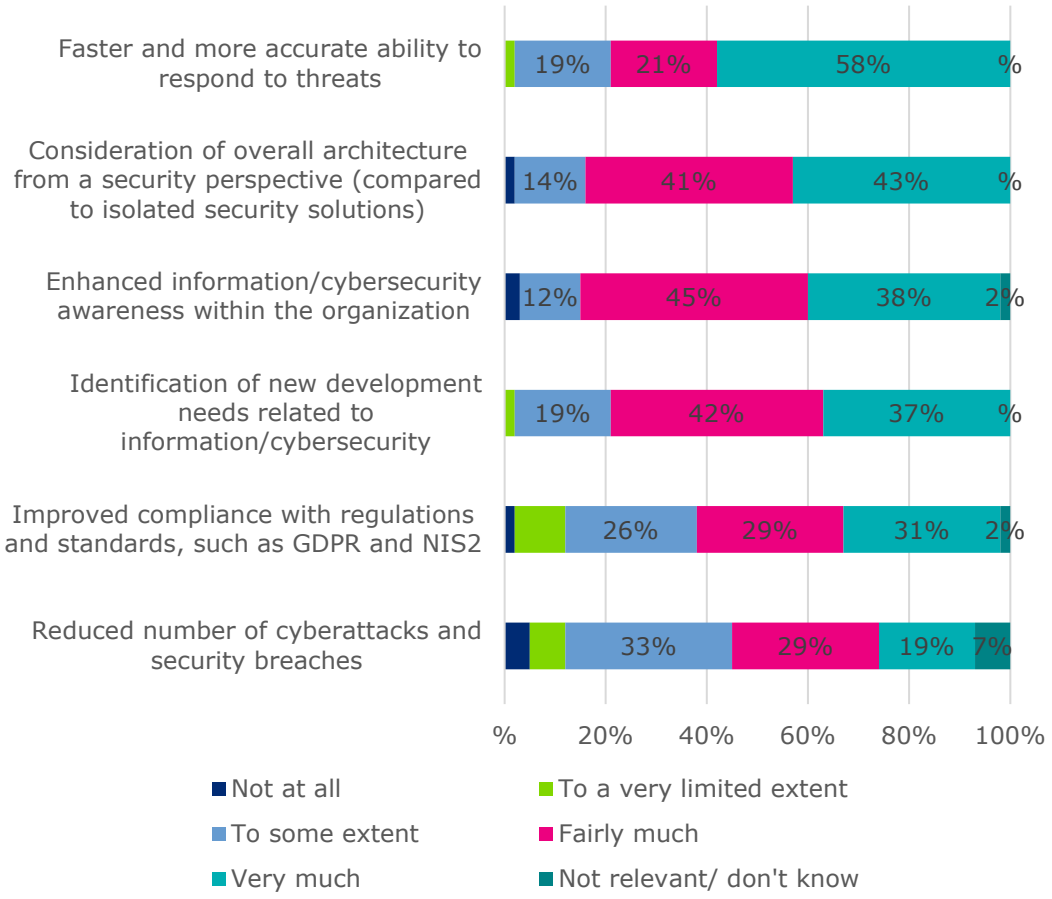

Figure 11. Question: To what extent has the organisation experienced (or are expected to experience shortly after the project's conclusion) direct and short-term benefits and outcomes from implementing information/cyber security solutions*? n=44 (N=50)*

The surveyed beneficiaries were asked to assess anticipated long-term impacts of the projects. The main anticipated impacts were related to enhanced resilience and ability to respond to new and complex cyber threats (84 % very or fairy much) and improved efficiency of information security and reduced manual work (78 % very or fairly much). Many of the respondents saw also potential positive economic impacts, namely increased customer trust and improved reputation (67 % very or fairly much) and achieving competitive advantage in the market (45 % very or fairly much).

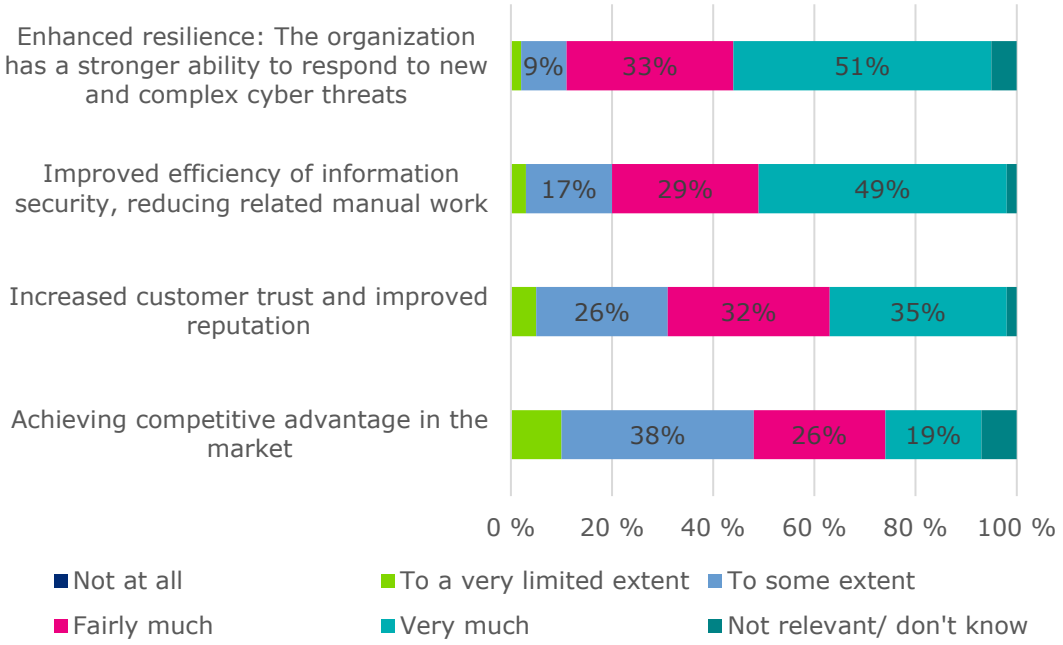

Figure 12. Question: To what extent has your organisation achieved or is expected to achieve the following long-term strategic benefits from the implementation of a state-of-the-art information/cyber security solution? *n=44 (N=50)*

Raising the maturity level of cyber security requires not only implementation of solutions but also the enhancement of skills, practices, and information exchange across the entire organisation. As reported by the beneficiaries, the support has had positive impacts on embedding cyber security within organisations. For the majority, the project has advanced cyber security-related expertise (76 % very or fairly much) and elevated the topic more prominently on management agendas (86 % very or fairly much).

In some organisations, expertise still needs to be disseminated more effectively to all employees through training and operational guidelines. Yet almost 70 % said that the project had supported organisation wide implementation (trainings, guidelines etc) and that security has become a part of the company's strategy.

Only about half of the companies have self-reportedly improved their ability to identify cyber risks across the entire supply chain (49 % very or fairly much). The sharing of information with stakeholders and partners should

be further strengthened, as more than 60 % reported that the project improved it only to certain or very limited extent.

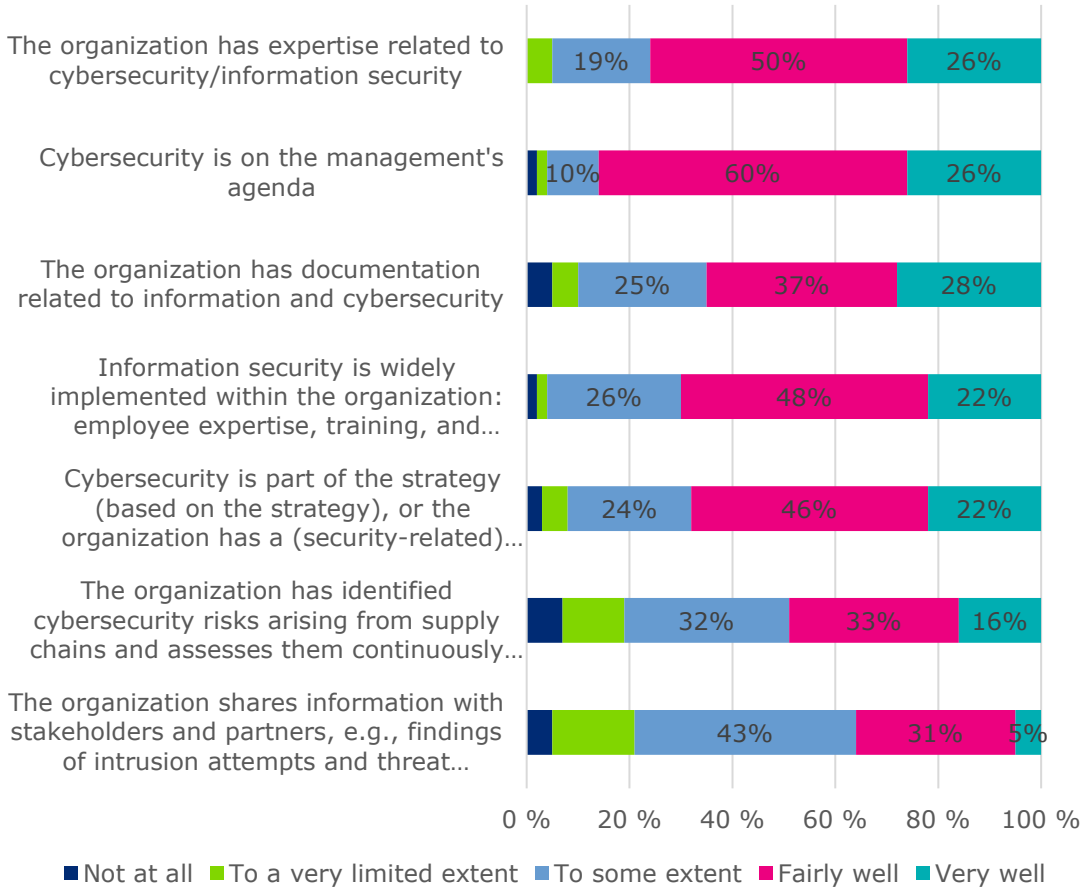

Figure 13. Question: To what extent has the project implemented with the support improved or advanced the following aspects in your organisation? *n=44 (N=50)*

3.2.4 Response to company needs

The support generally met the needs of beneficiaries exceptionally well. Over 90% of beneficiaries found the support to align excellently with their needs.

The most common criticism was related to the projects' timelines. Some suggested that the goals and criteria of the support could be clarified, and awareness of the support strengthened.

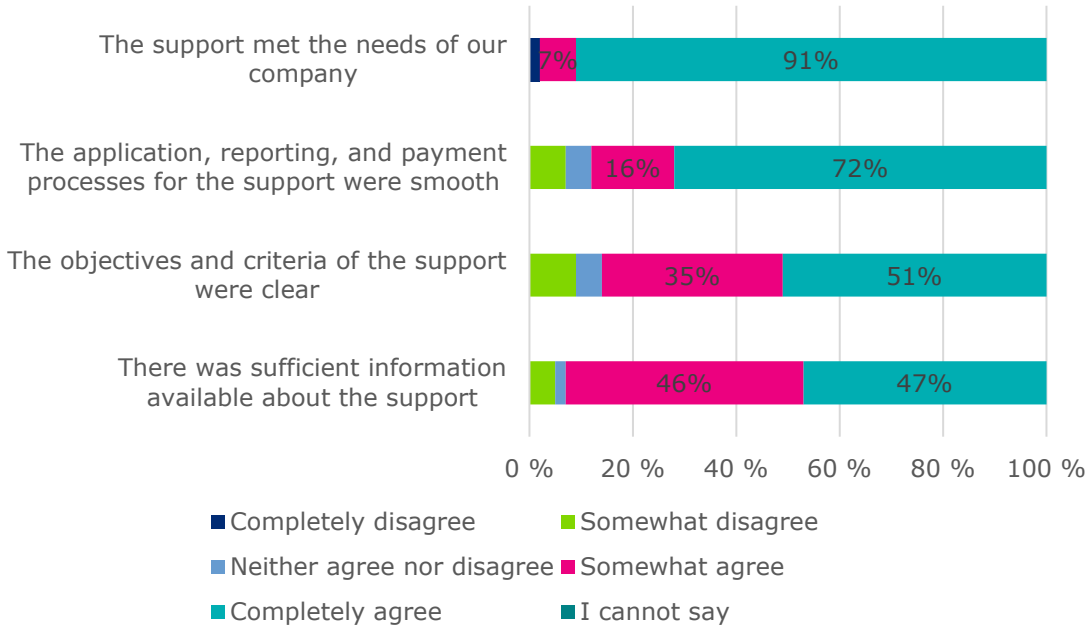

Figure 14. Question: Respond to the following statements. *n=44 (N=50)*

Sufficiency and conditions of the financial support (Survey, n=33)

The majority of respondents stated in the survey's open-ended answers that the financial support received was adequate for their project goals and allowed them to implement essential cyber security measures. While several respondents emphasised that the financial support was sufficient for their predefined objectives but mentioned that additional needs emerged during the project, which could not be covered within the allocated resources. Some respondents noted that while the financial support met the core project needs, additional resources would have allowed for broader or deeper improvements, such as testing, infrastructure upgrades, or addressing new requirements identified during the project.

A recurring theme was the challenge of project timelines. Many respondents found the project duration too short to complete all planned activities, suggesting that extending the timeline could improve outcomes.

Respondents appreciated the clarity and ease of the financial support process, including application and reporting requirements, describing it as less

bureaucratic. However, some suggested that allowing more flexible use of funds, such as for equipment or certification processes, would enhance their ability to achieve broader outcomes.

Many respondents expressed interest in additional financial support rounds to build on the progress made and address new cyber security needs as they arise. Continuous development of cyber security capabilities was noted as a long-term effort requiring sustained investment.

The responses generally reflected satisfaction with the financial support programme. Many acknowledged the significant impact of the financial support in enabling projects that would have been difficult or slower to execute otherwise. Respondents also recognised the value of finding suitable partners through the financial support initiative, setting the stage for future collaboration.

Challenges related to support and the project (n=33)

Overall, the respondents of the survey were satisfied and did not find many challenges related to the financial support or the project implementation.

However, a recurring theme was time constraints, with project timelines perceived as too short to allow for optimal implementation or thorough exploration. Delays in receiving financial support decisions often compressed the timeline, leading to rushed execution and challenges in prioritising tasks effectively. Suggestions included aligning project timelines with financial support approval dates to mitigate delays in project initiation. Many expressed the need for extended project durations to allow for proper planning, testing, and adjustments.

Respondents noted difficulties in balancing the demands of the supported project with other organisational priorities, particularly in small teams or resource-constrained settings. Some respondents mentioned that leadership and management constraints in smaller organisations limited their ability to allocate time and attention to the project. Respondents acknowledged that unexpected needs often emerged during the project, highlighting the importance of flexibility in scope and resources.

Few respondents had challenges with external partners, such as delays or mismatched capabilities, placed additional strain on project timelines and required organisations to adapt quickly.

This highlighted the need for strong project management and clear resource allocation from the outset.

Some respondents also mentioned complexity of the new technologies. Implementation of new technologies required significant time for preparation

and training, particularly when the technologies were unfamiliar to the organisation.

Despite the challenges, respondents generally found the process beneficial, with some describing the tight timelines as motivating. Many noted that the financial support and project structure ultimately delivered positive outcomes, even if adjustments were needed during implementation.

Strategies to further enhance cyber and information security in SMEs (n=27)

Financial support recipients highlight several key themes for promoting the adoption of state-of-the-art cyber security solutions in companies. The importance of financial support emerged as a recurring theme, with many respondents emphasising that financial support plays a decisive role, particularly for SMEs, which often have limited resources for cyber security investments.

A need for improving awareness and communication was also widely recognised. Awareness of the importance of cyber security solutions and concrete operational practices was generally perceived as weak, especially among SMEs. Suggested solutions included developing communication channels and training opportunities, such as webinars, case studies, and Traficom’s online courses. Analysing and sharing historical cyber security problems and incidents to help companies learn from others' experiences was also proposed. Additionally, creating common standards, rules, and recommendations could assist SMEs in understanding and comparing options more effectively.

To support the adoption of cyber security innovations in SMEs, respondents highlighted the importance of solutions being easy to implement. Small organisations often lack the personnel resources needed for large-scale project management. The value of ready-made example implementations was emphasised. Respondents also suggested focusing product development on usability and adoption support, as well as providing packaged and scalable solutions without overselling (e.g., "best reasonable practices").

Collaboration and expert support were frequently noted as critical for companies' cyber security development. Respondents stressed the importance of partnering with experts to ensure the implementation of tailored, need-specific solutions. Several pointed out the significance of carefully selecting partners to ensure the expertise and commitment of service providers. In terms of fostering collaboration among companies, many respondents suggested sharing best practices and experiences through forums or similar platforms.

3.2.5 Impact on competitiveness and competitive standing

According to Finnish Ministry for Economic Affairs and Employment, state aid for companies should have minimal distortive effects on competition. The financial support provided by NCC-FI is defined as a *de minimis* aid, i.e. it fulfils EU Commission's criteria for minor relevance to trade or competition in the common market.

The financial support's aims are mainly non-economical, related to improving companies cyber and information security maturity. However, 45 % of the beneficiaries of the financial support anticipated that the project will also help the company to get competitive advantage in the market (figure 15).

3.2.6 Impact with relation to company size, location and industry

Considering direct outcomes of the project, there were slight differences across company sizes, location and industries. The projects in Uusimaa region generally performed slightly worse than other regions in total, particularly in terms of providing training to personnel. Projects withing information and communications sector also performed slightly worse than other sectors on average, especially in cyber security assessments and training to personnel. Regarding company size, there was no significant trend to either direction and the differences were small.

In terms of results and anticipated impacts, there were no significant differences across the regions, sizes and industries.

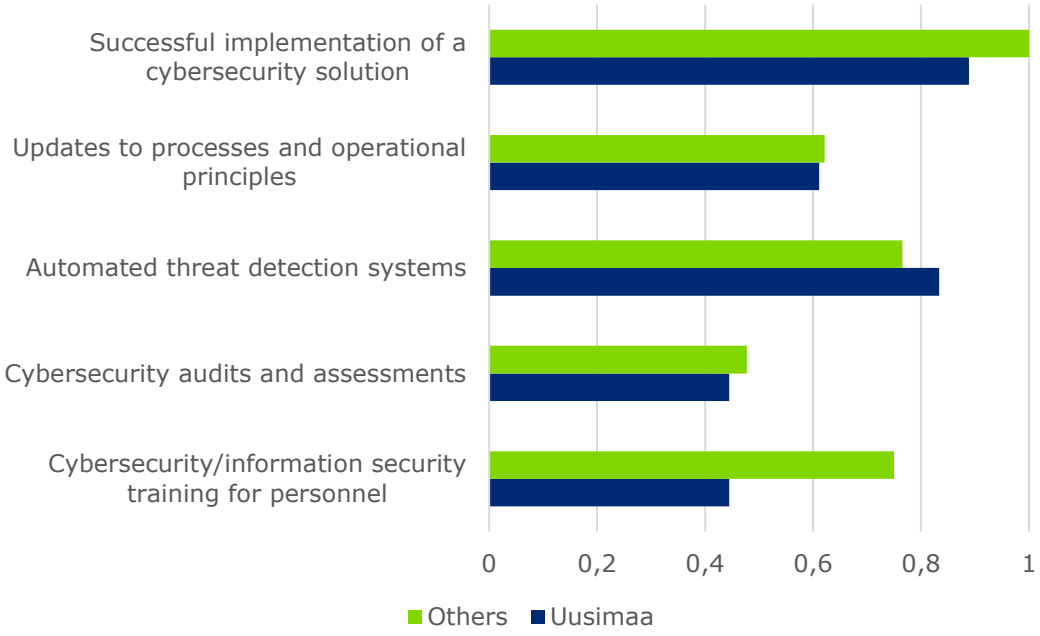

Figure 15. Question: What kinds of outcomes have been achieved in your company with the help of financial support? (You can choose multiple

options) *n=44 (N=50)*. Uusimaa region versus other regions. 1 = all companies, 0= none of the companies.

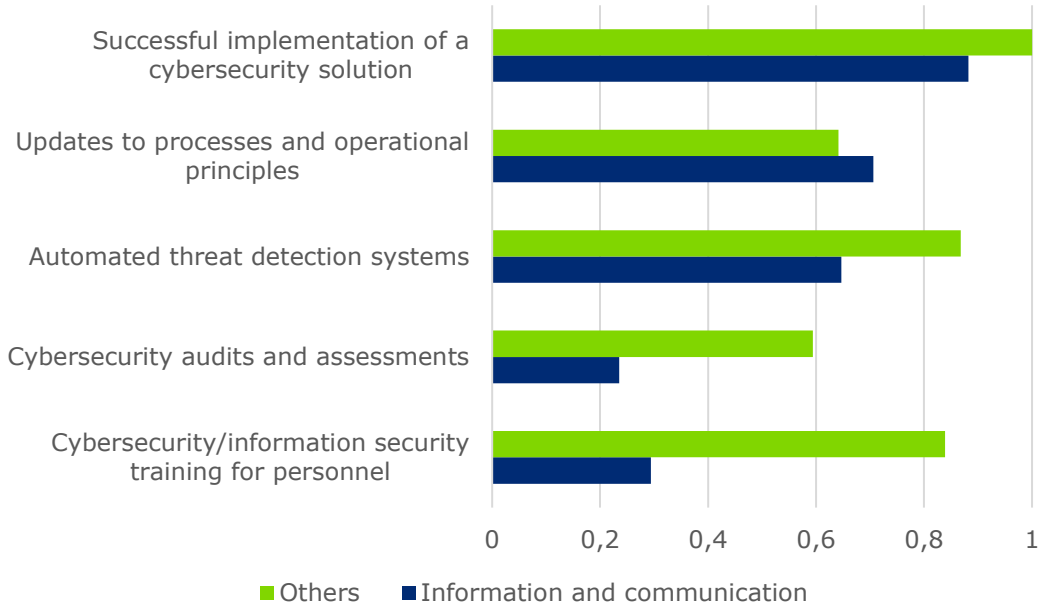

Figure 16. Question: What kinds of outcomes have been achieved in your company with the help of financial support? (You can choose multiple options) *n=44 (N=50)*. Information and communication sector versus other sectors. 1 = all companies, 0= none of the companies.

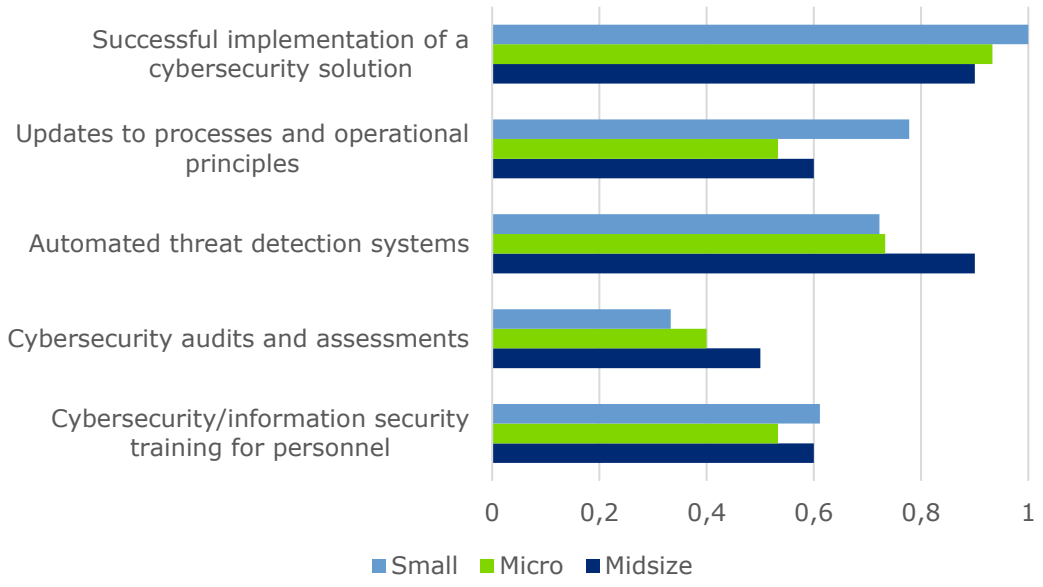

Figure 17. Question: What kinds of outcomes have been achieved in your company with the help of financial support? (You can choose multiple options) *n=44 (N=50)*. Micro, small and midsize enterprises. 1 = all companies, 0= none of the companies.

3.2.7 Summary of direct impacts

The beneficiaries reported that the financial support has significantly improved the cyber and information security of the recipient companies. Immediate benefits and results of the projects have been perceived as highly positive. The companies reported that the solutions were successfully implemented and additionally the beneficiaries enhanced their organisational skills, refining operational practices, and elevating cyber security as a priority on management agendas.

According to the beneficiaries, the projects have strengthened threat response capabilities, incorporated solutions to their comprehensive architecture, raised organisational awareness, and identified new development needs. Anticipated long-term impacts on cyber security include increased resilience (90% rated this as significant) and improved efficiency in information security measures (80% rated this as significant).

However, collaboration and information exchange could be further strengthened to amplify these benefits.

3.3 Indirect impact of provided financial support

3.3.1 Current state and needs of Finnish cyber security environment

The traditional strong level of cyber security in Finland is being challenged.

Finland's cyber security environment has become more challenging, dynamic, and the motivation factors for attackers increasingly diverse. Severe attacks are more frequently large-scale and prolonged APT (Advanced Persistent Threat) attacks. Perpetrators, such as in the attacks against Nordea, a large Nordic bank, in autumn 2024, possess extensive financial, technical, and skill-related capabilities. The resource usage observed in the case is difficult to justify with economic benefits, and although the attacker remains uncertain, it is likely politically motivated. Generally, this development raises the risk levels of attacks; when financial considerations do not limit the attacker, the duration and impact of the attack can significantly exceed the risk levels identified by the target.

Despite the challenges in the cyber security environment, Finland's corporate sector and broader society have traditionally achieved high international rankings in cyber security. Reasons for this include a high level of expertise, collaboration among security providers, the high quality of technology and service providers like telecommunications, disciplined operational principles, and the limited size of the language region. However, this situation may be changing, and Finland's lead narrowing. The primary reason for this is the globalisation and platformisation of technologies being used.

The growing significance of cyber threats impacts the entire society, businesses, and individuals due to digitalisation and technical advancement. Each entity's so-called attack surface is expanding and diversifying. Networked operating models increase the likelihood that successful attacks on one component will cause disruptions across the entire chain. This adds complexity to preparedness, technological diversity, skill requirements, and costs. The risks of networked operating models are well recognised, and EU-level NIS2 regulation provides a robust and concrete preparedness model, at least for critical societal actors.

Systemic preparedness is increasingly important

National risk management capacity includes production capacity (development side) and actions in other organisations (adoption of solutions and innovations). Overall, the state of the Finnish cyber and information security industry on the supply side is reasonably good. There is a lot of top-tier capacity, even comparing to the global level. However, vitality and business opportunities face challenges due to the general economic situation and consolidation of the market into the hands of few large multinational players. On the adoption side, Finland's performance is very good compared to

other nations. It boasts high competence and well-organised structures. However, the issue is that the level of cyber security across organisations is highly uneven. Especially SMEs are experiencing bottlenecks related to financing and skills to implement up-to-date security systems. Some public authorities and critical infrastructure companies excel, while other businesses are at a much lower preparedness level. These critical organisations compile only a small share of total businesses in Finland. As the modern-day risks are often systematic, it is not sufficient for national risk management capacity that only critical players are secured.

In terms of preparedness, it is no longer sufficient to acquire point solution services and technologies to specific situations that meet immediate needs, but rather consider the whole architecture. Comprehensive architectures[4] and systemic entities must be considered, along with understanding the offerings of major global players, their development, and often complex pricing structures. Previously, for example, malware protection could rely on standalone, possibly locally developed solutions. Now, integrating such solutions into cloud-based IT systems is often practical and, in some cases, even necessary to ensure seamless compatibility with the chosen architecture and technologies.

For the SMEs to meet the required security levels, the traditional (firewalls, antivirus etc.) solutions are no longer sufficient. While state-of-the-art technologies are important, the SMEs should adopt also state-of-the-art strategies on management models. State-of-the-art management models can be based on e.g., standards like ISO27001. It details requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS) – the aim of which is to help organisations make the information assets they hold more secure. Effective cyber security should be risk-based rather than solely technology-driven.

Individual companies as part of a system

The growing diversity of usage needs and systems also creates challenges for how a single organisation can improve its cyber security. Achieving the necessary security levels increasingly requires system-level and architectural changes, such as the implementation of the Zero Trust concept.[5] In this model, protections based on location and internal networks are

[4] Cyber security architecture is an essential part of a company's overall information systems architecture. It defines the structure of the organization’s security processes, cyber security systems, and personnel, as well as their relationship to the organisation's goals and strategic plans. A critical component of a cyber security strategy is the successful segregation of IT and OT environments.

[5] Zero Trust is a general framework that encompasses a variety of vendor-specific implementations. One example is Microsoft's approach, which is detailed at: https://www.microsoft.com/en-us/security/business/zero-trust

replaced with an assumption that the user has malicious intent. Therefore, user identity and access rights are frequently verified before granting access to the system. The model offers undeniable benefits when using cloud services regardless of location, thereby supporting remote work and its security. However, implementing the concept is heavy and typically requires significant changes and investments in IT and cyber security architectures. Justifying these changes to company leadership and possibly the board can be considerably more challenging compared to earlier, more isolated and concrete cyber security investments. In general, financially justifying cyber security investments is challenging since it is an insurance-type investment, where the likelihood of risk realisation is perceived as low, and assessing the overall impact is difficult.

Broad cyber security solutions impact the entire company. The implementation of comprehensive cyber security solutions affects the entire company, including its processes, responsibility definitions, and data classification. To achieve the intended level of security, many fundamentals must be in place. For example, the adoption of Zero Trust concepts heavily relies on proper identity and user management. This is reflected in the demand for IAM (Identity and Access Management) services and consultants. Finland has traditionally excelled in IAM expertise, both in terms of its own products and service offerings.

Global-level consolidation in development of cyber security solutions poses both opportunities and threats

As mentioned above, the production capacity of cyber security solutions is being transformed as large-scale multinational players (e.g., Microsoft) are taking up larger and larger share of the global market. They offer integrated security solutions, often tied to digital services like Teams. While this is logical and efficient from the perspective of SMEs, over-reliance on one provider is not adequate for state-of-the-art cyber security needs. On the one hand, selecting and essentially committing to the offerings of a major global provider, such as Microsoft, provides customers with security and access to an extensive range of cyber security solutions. However, this comes with a significant price tag, which may be unaffordable for many SMEs and even larger enterprises. Licensing fees for global providers like Microsoft are substantial, and customers often have limited bargaining power in price negotiations. Additionally, understanding and anticipating product roadmaps, packaging, and pricing structures require substantial expertise and time investment, further adding to costs. On the other hand, the cost of disengaging from such providers can be significant and time-consuming. For geopolitical and self-sufficiency reasons, there is also a need for ensuring that EU-based and domestic solutions are available. Diversification would be advisable.

A broad systemic approach, however, offers an excellent opportunity to leverage new state-of-the-art technologies and integrate them in a controlled and well-aligned manner. Developing advanced technologies, such as artificial intelligence, requires considerable resources. As a result, their development and integration into product and service ecosystems increasingly rest in the hands of large global players. While the drivers of technological development, such as generative AI, may not directly relate to cyber security, this development also has implications for security technologies. It enables the creation of increasingly sophisticated and faster attacks while assisting in the detection of such attacks. Therefore, elements of AI development are almost mandatory for security products and services to maintain previous security levels. In traditional network-level cyber security, AI-like algorithms have long been developed and used to identify harmful anomalies in network traffic. The latest AI developments present further opportunities to advance these systems.

Globalisation and the offerings of large players are at the same time levelling the playing field. The development described above also means that the solutions used by companies are becoming standardised, reducing national differences. While Finland has traditionally been a pioneer in the development and application of cyber security technologies, at least on a European scale, this is becoming increasingly challenging. Organisations and their systems are now more likely to have the same vulnerabilities as others. If an organisation aims to invest in and develop security to surpass its peers, the targets of such investments are increasingly controlled by others, such as global cloud service providers. Customers' ability to influence the security levels, processes, and controls of cloud services is very limited.

The cyber security market is growing rapidly

The global market for cyber security products and services was estimated at EUR 160 billion in 2023 and is expected to grow to EUR 523 billion by 2032, representing a significant annual CAGR of 14.3 %. The services market is growing faster than the product market, with a CAGR of 20.2%, reaching EUR 61.7 billion.[6]

Finland's total cyber security market is estimated to be €1.3 billion.[7] Based on the membership of FISC (Finnish Information Security Cluster), there are approximately 50 cyber security-focused companies in Finland.[8] An increasing number of companies operating in Finland are service providers. This is due to the previously described development, where large global

[6] Fortune Business Insight https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165
Last Updated: October 07, 2024 Report ID: FBI101165
[7] FISC ry, Finnish Information Security Cluster
[8] FISC ry, Finnish Information Security Cluster

cyber security providers such as Palo Alto Networks, Fortinet, Cisco, Microsoft, and Crowdstrike have made numerous acquisitions and aim to capture an increasing share of customer budgets. This leaves less room for smaller, more niche players. On the other hand, the importance of national service providers may grow in customers' cyber security strategies because the integration and management of products are becoming increasingly challenging as digitalisation expands and cyber security products and services diversify.

3.3.2 Impact on companies in the cyber security sector

As discussed in the earlier chapters, there is a global development where the production of cyber security solutions is being consolidated to large-scale multinational companies. While this development provides several opportunities, it also poses certain threats to national self-sufficiency. The Finnish cyber security industry offers some globally competitive solutions, but this is partly being challenged by the consolidation. A growing share of Finnish cyber security firms are nowadays service providers instead of developers of solutions.

Overall, the market impacts of the financial support are expected to be small, as the volume of the financial support is small comparing to the size of the market. The total financial support was EUR 2 million for 2 years excluding beneficiaries' own investments. The projects were purchasing services with approximately EUR 1 million and other purchases and licenses with EUR 0.2 million euros. Finland's total cyber security market is estimated to be EUR 1.3 billion.[9]

The analysed project reports reveal that the beneficiaries were buying international solutions and national services for integration and other support activities. According to the project plans, EUR 0.8 million were directed to purchasing services, which were mainly purchased from Finnish IT service companies (EUR 0.1 million unspecified) and EUR 0.1 million to foreign owned companies producing the solutions and innovations. The solutions providers include e.g., Microsoft, Sophos, Crowdstike and Amazon. Some Finnish solutions were used as well (EUR 31 thousand euros), namely WithSecure. While the increased demand on cyber security solutions is very low measured in euros, the financial support does stimulate the Finnish IT service market to some extent. However, it must be noted, that integration services are likely to be one off purchases, whereas most of the solutions function on licence-based model. Assuming that the beneficiaries continue to use the solutions, they adopted during the project, the lifetime stimulus for cyber security solution market will be significantly larger.

[9] FISC ry, Finnish Information Security Cluster

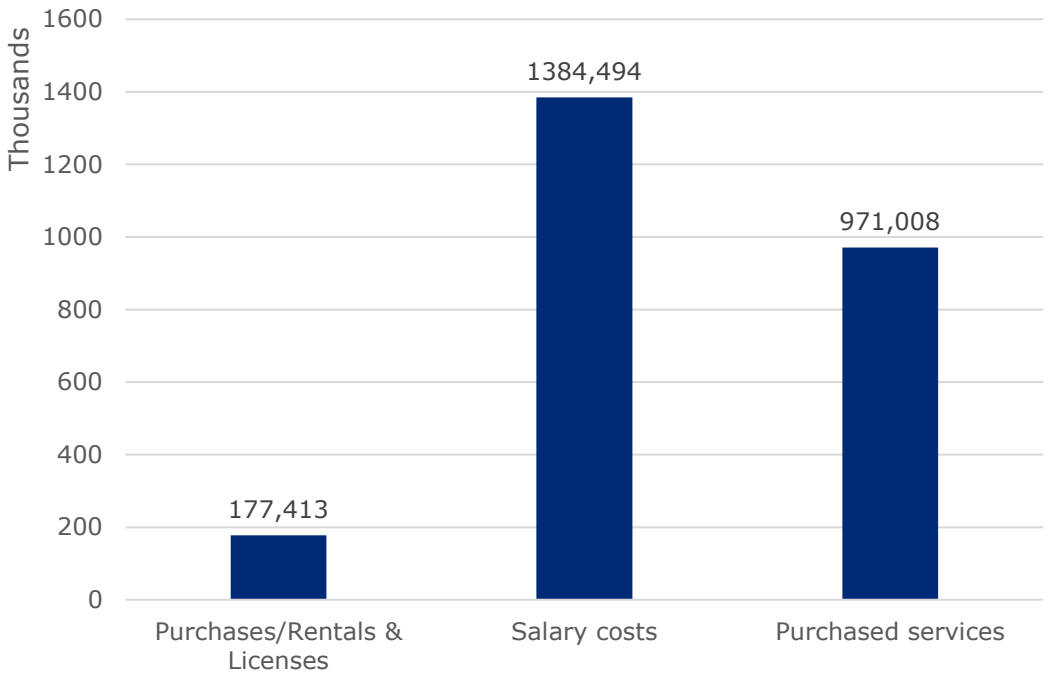

Figure 18. Cost structure of projects. The analysis is based on salary costs, purchased services, purchases, and licenses reported in the final reports.

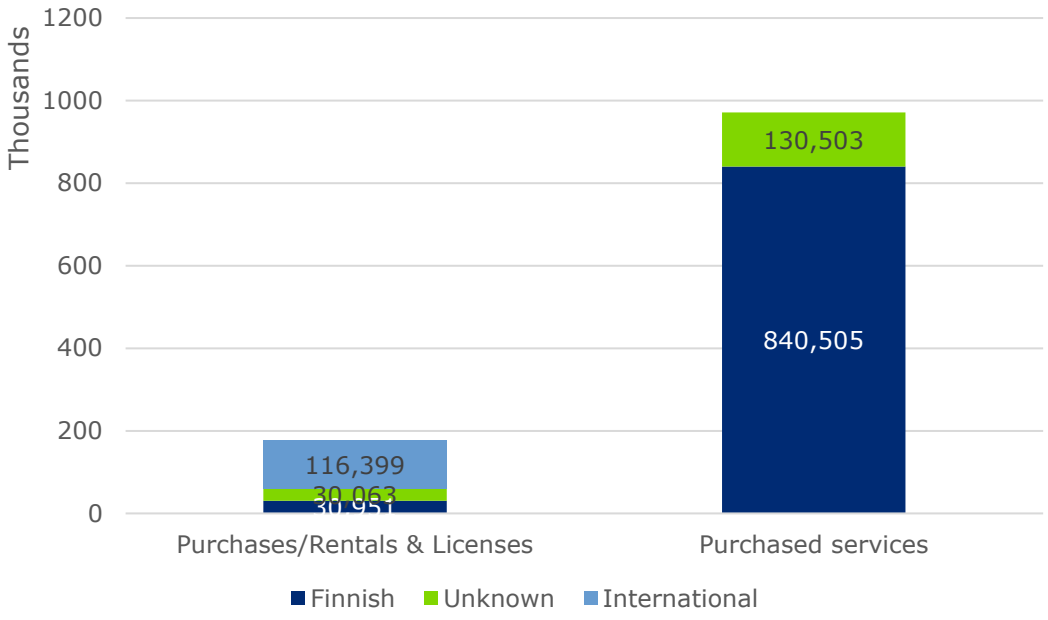

Figure 19. Country of origin of purchased services and solutions. The analysis is based on purchased services, purchases, and licenses reported in the final reports. Unknown = The service or technology provider was not specified.

3.3.3 Impact on other companies

Critical sectors form the backbone of society. The cyber security of companies operating in these sectors directly affects societal functionality, including supply chain reliability and the management of disruptions. SMEs, can be linked to critical organisations though their clients or supply chains. If a

company's clients operate in critical sectors, the clients' data security is indirectly dependent on the partner company's level of security. Therefore, adoption of state-of-the-art solutions in SMEs can significantly enhance customer security and overall national cyber security capacity.

The financial support does not have criteria for targeting support to critical or other sectors. However, the findings of the evaluation show that the financial support has been mainly utilised on the information and communication technology sector, health care, digital services and digital infrastructure. The beneficiaries have linkages (e.g., via customers or supply chains) to sectors, that are considered in NIS2 regulation as highly critical, such as energy. This way, the financial support may have indirect positive spillover effects to critical sectors and impact beyond the beneficiaries themselves.

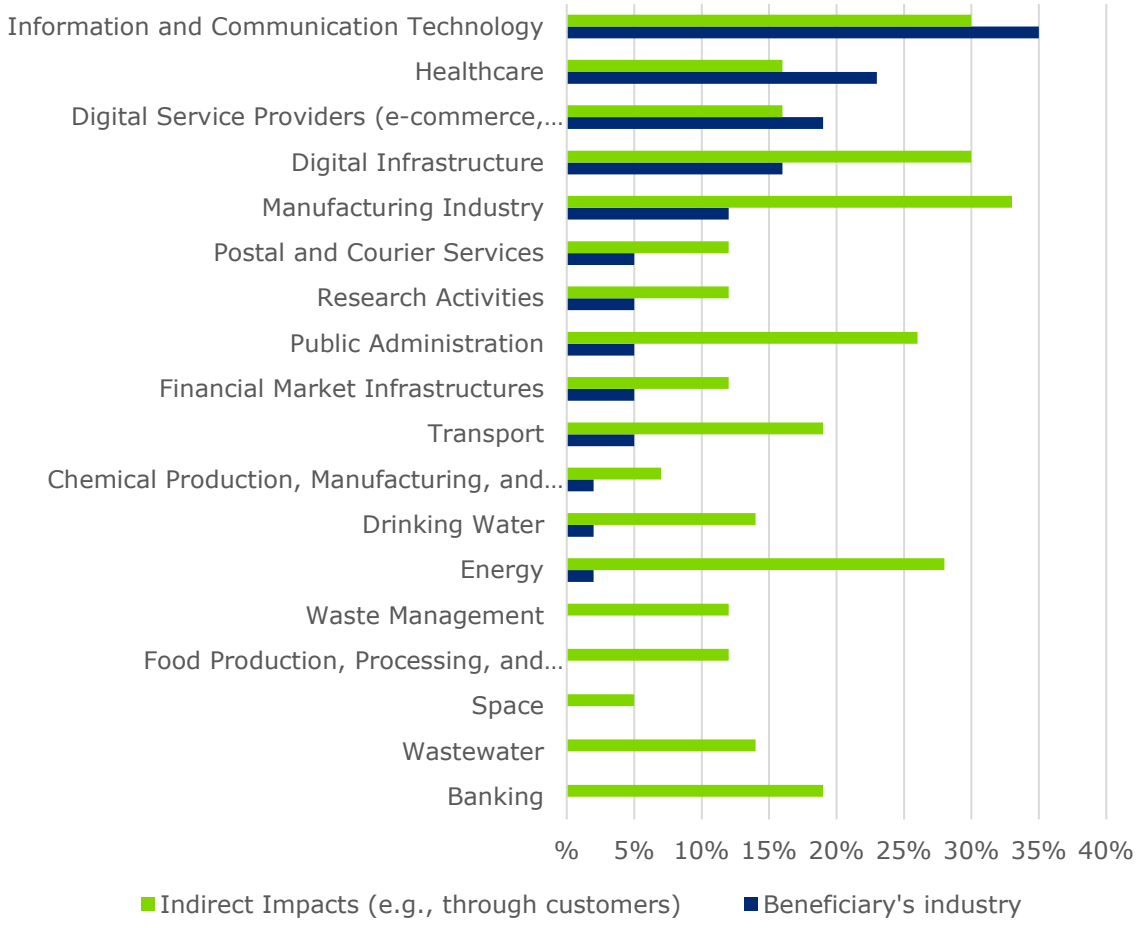

Figure 20. Question: Does your organisation 1) operate in any of the following industries, or 2) indirectly impact the cyber security of organisations in these industries (e.g., through a customer relationship)? *n=44 (N=50)*. The classification is based on the categorisation of critical sectors outlined in the NIS2 Directive.

3.3.4 Impact on the cyber security capacity of the Finnish society

In terms of national preparedness, it is no longer sufficient that companies acquire point solution services and technologies to specific situations that

meet immediate needs, but rather consider the whole architecture. For the SMEs to meet the required security levels, the traditional (firewalls, antivirus etc.) solutions are no longer sufficient. While state-of-the-art technologies are important, the SMEs should adopt also state-of-the-art strategies on management models. State-of-the-art management models can be based on e.g., standards like ISO27001. Effective cyber security should be risk-based rather than solely technology-driven. By adopting state-of-the-art solutions, SMEs can impact the cyber security capacity in national level, as many of the modern-day risks are systemic. A weak link in a system can cause system wide threats.

Acknowledging that some of the nation-wide cyber security issues stem from outdated technologies in use, the financial support was targeted to up take of state-of-the-art cyber and information security solutions and innovations. While the definition of a "state-of-the-art technology" is difficult to define, NCC-FI uses some rough guidelines. It is mentioned in their website that "A state-of-the-art solution or innovation to be adopted represents relatively new and advanced technology. State-of-the-art solutions leverage, for example: advanced automation, machine learning, artificial intelligence, encryption solutions resilient to quantum technology, or new network technologies (such as SDN, SD-WAN, or 5G). Solutions that have been in use for a long time, such as traditional firewalls, antivirus programs, or virtual private networks, are not considered state-of-the-art solutions." Furthermore, if traditional solutions are implemented in a novel and advanced way, they can also be considered.

Based on this rough definition, the project plans and report were analysed to understand what type of technologies the projects were adopting. Majority of the technologies were indeed state-of-the-art, while there were some traditional solutions involved as well. Most of the projects were up taking more than one solution and some solutions may involve more than one the following categories.

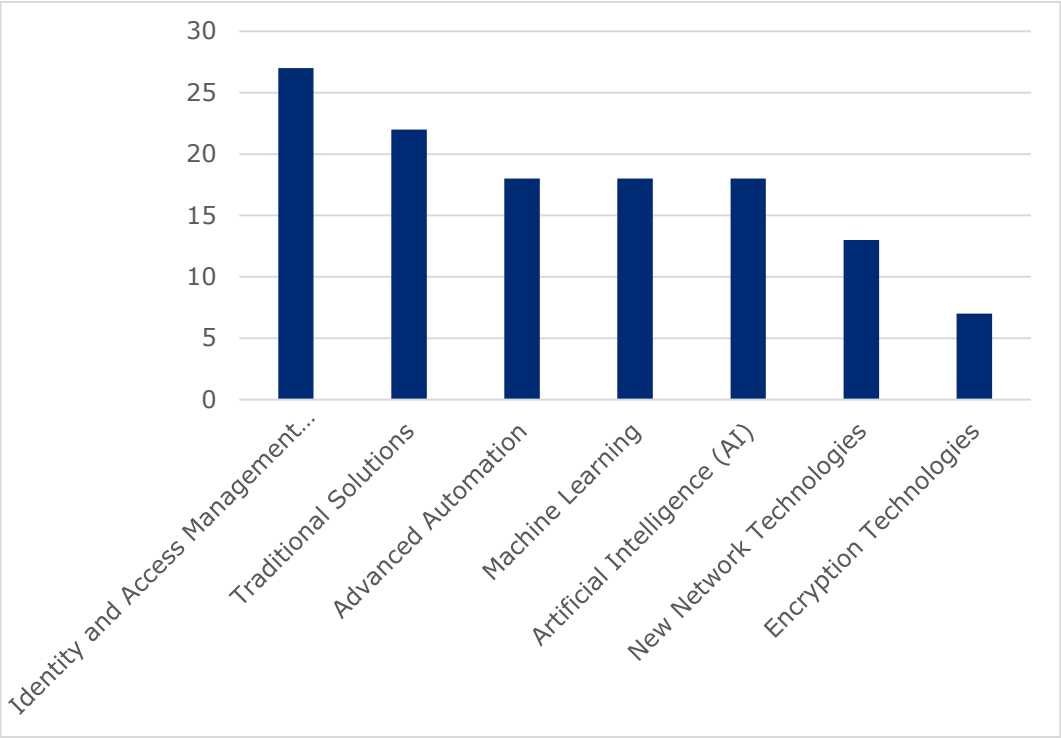

Figure 21. The classification is based on the technologies or solutions mentioned in project plans. One project plan may involve multiple technologies and categories. Only projects that received financial support are included in the classification.

Table 5. List of analysed technologies and their classifications.

Technology
Advanced Automation E.g., RPA (Robotic Process Automation), Automated Threat Detection
Identity and Access Management (IAM) Biometric Authentication, Multi-Factor Authentication (MFA), Zero Trust Architecture
Machine Learning Anomaly Detection, AI-Based Phishing Detection, Machine Learning-Based Threat Analysis
Traditional Solutions Firewalls, Antivirus Programs, or Virtual Private Networks (VPNs), implemented with innovative approaches
Encryption Technologies End-to-End Encryption, Homomorphic Encryption, Blockchain Technologies in Cyber security
Artificial Intelligence E.g., AI-Based Threat Prediction, Automatic Vulnerability Scanning, Honeypots and AI-Based Disruption, Intelligent Identity Management
New Networking Technologies Software Defined Networking (SDN), Software Defined Wide Area Networking (SD-WAN), 5G Security Features, Multi-Access Edge Computing (MEC)

3.3.5 Impact on the Finnish and European strategic autonomy and competence in the area of cyber security

From the perspective of nation and EU wide cyber competence, it is crucial that improvements in cyber security are being implemented in all businesses, not only the frontrunners. As discussed earlier, one issue in Finland

is that there are wide differences across businesses on their preparedness. The nation-wide capacity requires that all businesses improve their capacity. Therefore, it is well justified that the financial support is targeted to micro companies and SMEs, which typically have investment and skills barriers in adopting new cyber security solution. Supporting companies that fall behind in adopting state-of-the-art cyber and information security solutions benefits the entire society, not just individual businesses. It increases societal resilience, enhances ecosystem security, levels the competitive playing field, strengthens critical infrastructures, and reduces economic and social risks. Additionally, improvements in nation-wide cyber security can improve Finland's reputation as a secure and reliable player on a global level, particularly from an investment perspective.

The evaluation was comparing the beneficiaries' survey results to Eurostat's statistics on ICT security measures on Finnish companies. As there is large sectoral variance on the measures used, the evaluation was using the beneficiaries top3 sectors as a comparison group (ICT, professional and scientific activities and manufacturing). The results show (figure 22), that the beneficiaries were lagging their sectoral counterparts in several measures, most drastically in monitoring systems, ICT security testing, and user authentication solutions. However, based on the survey results, the projects improved adoption of those security measures that the companies were lacking before the financial support.

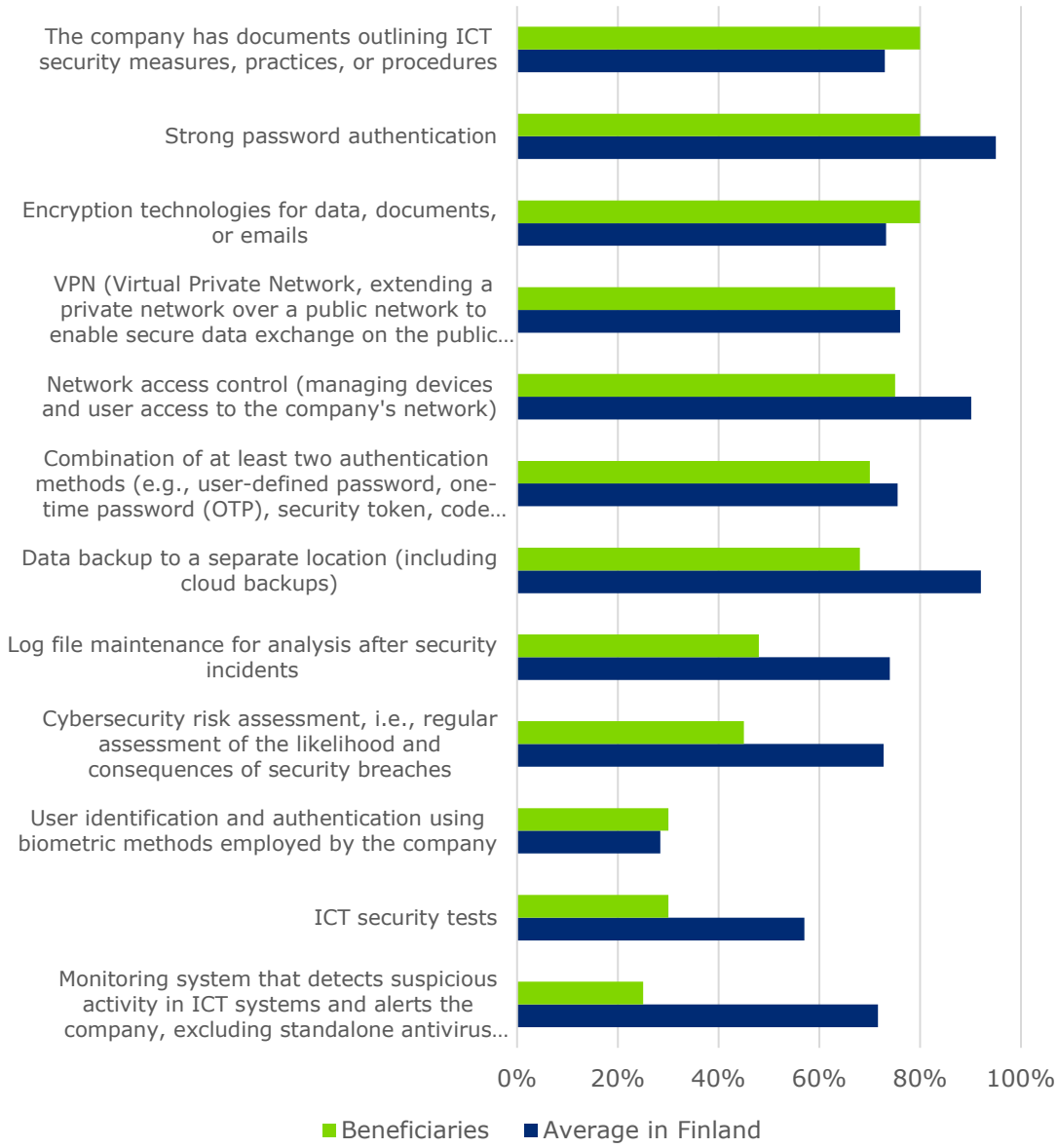

Figure 22. Question: Which of the following information/cyber security-enhancing measures were in use before receiving the support? *n=44 (N=50)*; Finnish average is based on ICT, and professional, scientific, and technical activities and manufacturing sectors, which were also the most common sectors among the support recipients. Source: Eurostat, ICT security in enterprises.

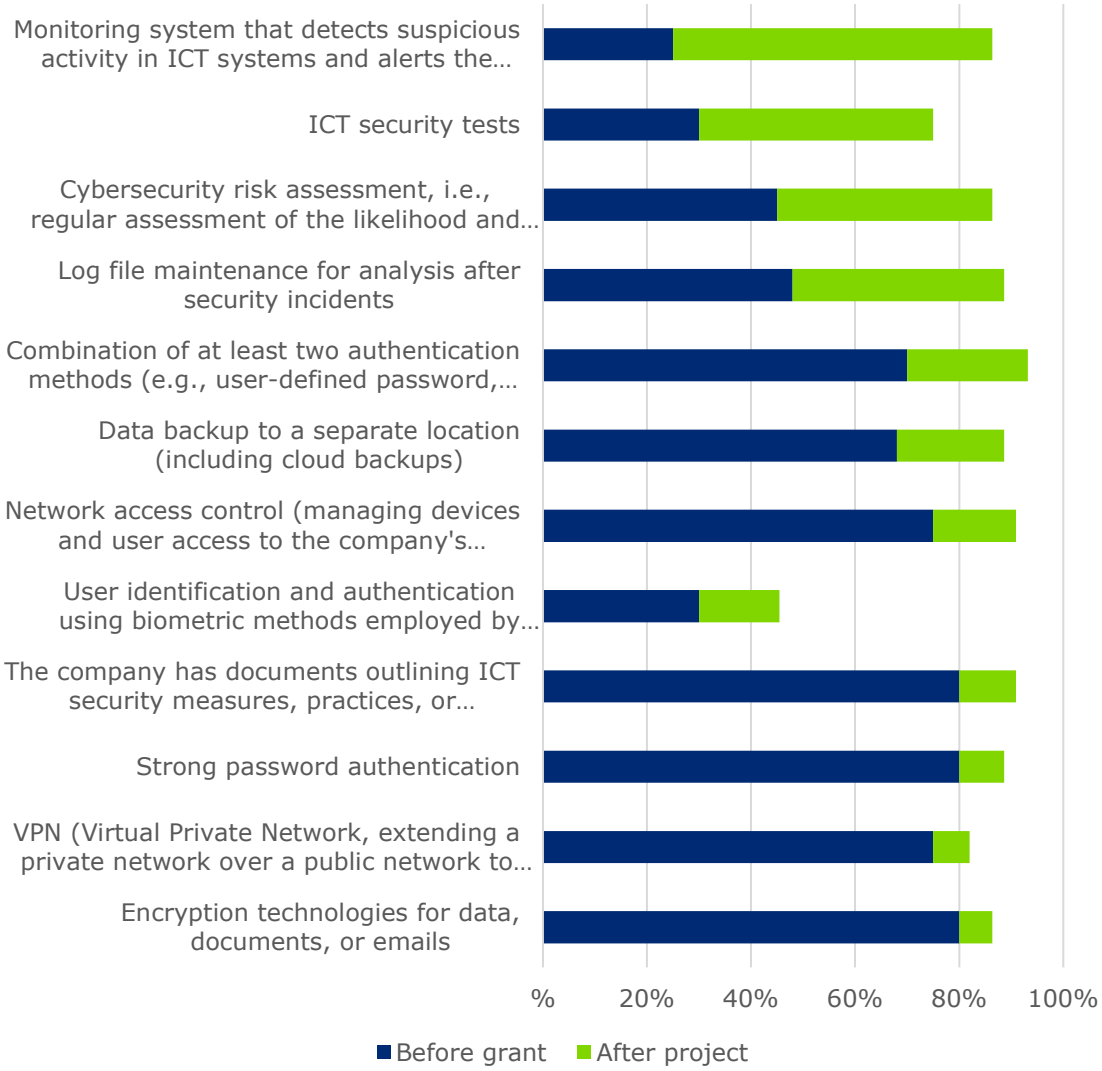

Figure 23. Question: Which of the following information/cyber security-enhancing measures were in use 1) before receiving the support and 2) after the project has been finalised? *n=44 (N=50)*

3.3.6 Summary of indirect impacts

As the total volume of financial support is quite small (EUR 2 million) comparing to the size of the market and the needs of SMEs, the accumulative indirect effects of the financial support are assessed to be small. However, the support has been targeted in a way that is effectively having positive spillover effects and indirect impacts.

The financial support has primarily been allocated to companies operating in the ICT sector, but many of these companies have customers in critical sectors (e.g., banking, energy).

The financial support has enabled the adoption of state-of-the-art solutions that offer significant advantages over traditional, isolated solutions. These solutions can improve the resilience of the entire network as they integrate into it.

From the perspective of overall impact, it is well justified to direct financial support to companies with deficiencies in cyber security. Companies that have received financial support have had weaker cyber security capacity compared to the average level of Finnish companies, as shown when comparing survey and Eurostat data. Targeting small and medium-sized enterprises (SMEs) is also well justified.

Due to the limited amount of financial support, its market impact has been small. The financial support has slightly (EUR 1.1 million) increased demand for domestic services, but the implemented solutions have predominantly been provided by multinational companies on license basis.

4 Conclusions and recommendations

4.1 Conclusions

A) Direct and short-term impact of the financial support

The financial support has well fulfilled its purpose and its direct impact to beneficiaries can be considered high.

Technically all projects (95 %) stated that they have successfully implemented their technology upgrading and reached the project goals. Besides adoption of the technology, the companies have organised training for staff and developed internal processes and documentation. The companies are also reporting increased resilience against cyber-attacks.

Some companies reported that during the course of the project, they had also identified additional security issues to be addressed.

Furthermore, beneficiaries were conducting also actions that were not primarly targeted in the call for proposals document, such as trainings for staff and sharing of information and experience with other companies. This is an indication that the financial support has triggered some behavioural changes and new practices with longer-term impacts. Staff training and peer-to-peer knowledge sharing are eligible costs for projects.

There is a clear additionality of the financial support. Most beneficiary companies reported that they would have not implement the project at all, or in a similar scale without having received the financial support and that the financial support had sped up their actions to improve cyber security. In particular SMEs and micro enterprises are facing investment and skills barriers with regard to cyber security upgrades. The financial support has managed to alleviate both. The necessary expertise was usually procured from external service providers.

All in all, it appears the support has met the needs of the beneficiaries to a great extent. The recipients reported that the amount of the financial support was sufficient and in general, the terms, conditions and application processes were appropriate. The only issue was regarding the timeline, which was considered too tight by most beneficiaries.

B) Short and long-term indirect impact

It appears that the support has had, at least to some extent, positive impact on beneficiaries' competitiveness more generally. Many companies (80 % said fairly or very much) report that the projects have made their security functions more cost-effective, had a positive impact on their reputation and customer trust (70 % said fairly or very much) and have given some

competitive advantage also in the market (50 % said fairly or very much). There is however little concrete evidence on the scale of this impact.

The financial support has also generated some additional demand for the provision of IT services with the volume of around EUR 0.9 million. Comparing this to the size of the domestic service market (~EUR 1.3 billion), this impact is quite small and rather temporary. The purchased technological solutions were mainly those provided by international large-scale companies. The demand was increased by 180 000 euros during the project time span, but as most of them are license based, the lifetime cost will be higher.

As the state-of-the-art IT systems are strongly interconnected, also cyber security upgrades generate positive spillovers to other companies (e.g. to collaborators, subcontractors, clients). It is not enough that there are few market leaders in security, but every part of the chain or ecosystem must meet the security needs. Typically, particularly smaller enterprises have lower capacity to address security issues. This network effect is both impacting other companies and improving the overall capacity to address security issues.

Based on the survey and in reflection to Eurostat statistics, the NCC-FI financial support beneficiaries represent those industry sectors that were using overall less ICT security measures than companies on average in Finland before the financial support. This suggests that the NCC-FI support was granted to companies that are in need for technological upgrade.

According to the survey, most of the companies reported that the projects have put cyber security more strongly into management’s agenda, which is a good predictor that the impact will sustain beyond the project life cycle.

Considering national cyber capacity, there is a need for companies to share their cyber threat information and best practices with each other. Some of the beneficiaries were reporting that they started to share information during the project and many of them understood the benefits of doing so. However, more work could be done to incentivise companies to share information and collaborate in larger scale.

From the perspective of Finnish and EU-wide cyber self-sufficiency, there is a threat that current solutions and innovations are predominantly made outside EU. The solutions that were adopted in the projects were largely international solutions. While it might be problematic to directly mandate the support to nationally produced solutions, there is room for sharing information and knowledge about native options.

C) *Proportionality and appropriateness*

It seems clear that the limited volume (EUR 2 million) of provided financial support is not enough to address the cyber security challenges of Finnish enterprises at large. The volume is appropriate either as a targeted support and incentive to address certain identified challenges.

The grant size (max EUR 60 thousand) could be equally effective in a slightly smaller form (e.g. EUR 20 thousand), thus allowing for more grants to be delivered. This could increase the impact and spread awareness. Overall, the companies were reporting that the individual grant sizes were sufficient for implementing the project.

The type of financial support (grant-based co-financing) is typical and probably the most suitable form of financial support for these kinds of investments by companies. In particular, when Traficom also provides alternative voucher-type of financial support separately. Other possible forms, such as tax incentives or loan financial support would be more difficult to administer, target (tax incentives) and to apply for, and would probably better suited for larger and longer development projects with technological risks to be shared.

Experience from other evaluation suggest that financial support is more effective when complemented with non-financial support, in particular technical assistance or professional guidance. This would appear a relevant option to consider in the case of cyber security too, where technological choices play an important role in system upgrades.

4.2 Recommendations

1. There appears further need to support the upgrading of cyber security solutions of Finnish companies with financial incentives. NCC-FI should aim to continue its efforts to this end and pursue relevant financial support for it from European and national sources.

2. The effectiveness of the instrument could most likely be increased by decreasing the size of individual grants, while expanding the number of given grants. This would widen the reach of support to additional beneficiaries.

   The support has been very attractive and not all applicants have received financial support. In terms of national cyber security capacity, it is important to ensure that all businesses, also the non-critical ones, have sufficient security level and are prepared to meet the necessary regulations (NIS2). Hence, there is a need to raise the awareness, competence and cyber security level of the business sector, as a whole.

3. The instrument should better support holistic approach to cyber security and encourage companies to take actions beyond adoption of technology, e.g., training staff, conduct company specific risk assessments, exchange information and collaboration with other companies regarding cyber threats and best practices.

4. The financial support should be complemented with non-financial support, such as technical guidance and sharing of good (process) practices, to enhance its effectiveness. In particular, the lesson and practices from other NCCs should be systematically collected and applied.

List of references

European Commission (2020). Joint Communication to the European Parliament and the Council. The EU's Cybersecurity Strategy for the Digital Decade. JOIN (2020) 18 final.

European Parliament (2016). Directive (EU)2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148

European Parliament (2021). Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres.

European Parliament (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972 and repealing Directive (EU) 2916/1148 (NIS 2 Directive)

Liikenne- ja viestintäministeriö (2021). Kyberturvallisuuden kehittämisohjelma. LVM publications 2021:7. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/163219/LVM_2021_7.pdf?sequence=1&isAllowed=y

Traficom (2019). Digital Europe funding application for project 101100631 "Building Capacity for the Finland National Coordination Centre for Cybersecurity in Industry, Technology and Research". Confidential.

Valtioneuvosto (2018). Laki Liikenne- ja viestintävirastosta 23.11.2028/935

Valtioneuvosto (2019). Suomen kyberturvallisuusstrategia 2019. Valtioneuvoston periaatepäätös PLM/2019/52.

Valtioneuvosto (2024). Finland's Cyber Security Strategy 2024-2035. Valtioneuvoston kanslian julkaisuja 2024:11

Finnish Transport and Communications Agency Traficom
PO Box 320, FI-00059 TRAFICOM
Switchboard: +358 29 534 5000

traficom.fi

ISBN 978-952-311–592-9
ISSN 2669-8781 (e-publication)

TRAFICOM
Finnish Transport and Communications Agency