

GEIGER

The logo for Geiger, featuring the word "GEIGER" in a bold, black, sans-serif font. To the right of the letter "R" is a stylized green icon consisting of three concentric, slightly irregular circles, resembling a geiger counter's detection pattern.

Deliverable

D5.1 | Impact Plan

Point of Contact | Heini Jarvinen

Institution | Fores Media Limited (Tech.eu)

E-mail | heini@tech.eu

Phone | +32 456 22 59 15

Project Acronym	GEIGER
Project Title	GEIGER Cybersecurity Counter
Grant Agreement No.	883588
Topic	H2020-SU-DS03
Project start date	1 June 2020
Dissemination level	Public
Due date	M06
Date of delivery	30/11/2020
Lead partner	TECH.EU
Contributing partners	UU, TECH.EU, KASP, PHF, MI, KPMG, BBB, ATOS, KSV, HAAKO, CERT-RO, CLUJ IT, E-ABO, SCB, PT, SRA, CL
Authors	Heini Jarvinen (TECH.EU), Samuel Fricker (FHNW), Stelian Brad (CLUJIT)
Contributions	Helen Walsh (TECH.EU), Cédric Merz (FHNW), Mia Braunwalder (FHNW), Alireza Shojaifar, FHNW, Bettina Schneider (FHNW), Jessica Peichl (PFH), Bernd Remmele (PFH), Marco Spruit (UU), Amedeo D’Arcangelo (KPS), Cristian Priboi (CERT-RO), Dumitru David (CERT-RO)
Reviewers	Euplio Digregorio (SKV), Nuria Rodríguez (ATOS), David Elfassy, Lior Armive (KPMG)

This document contains information that is treated as confidential and proprietary by the GEIGER Consortium. Neither this document nor the information contained herein shall be used, duplicated, or communicated by any means to any third party, in whole or in parts, except with prior written consent of the GEIGER Consortium.



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

Revision History

Version	Date	Author	Comment
0.1.1	28/10/2020	Heini Jarvinen, TECH.EU Cédric Merz, FHNW Mia Braunwalder, FHNW Jessica Peichl, PFH Bernd Remmele, PFH Helen Walsh, TECH.EU	T5.1 Dissemination and MSE ecosystem-building Website, newsletter mailing list Logo, style guidelines, templates GEIGER Education GEIGER Education Editing, stakeholder mapping
0.2	28/10/2020	Samuel Fricker, FHNW	Introduction T5.2 Standardisation and liaison with policy
0.3	29/10/2020	Stelian Brad, CLUJIT	T5.3 Exploitation planning
0.4	30/10/2020	Heini Jarvinen, TECH.EU	Executive summary
0.5	04/11/2020	Alireza Shojaifar, FHNW Marco Spruit, UU	T5.1 Dissemination and MSE ecosystem-building, Academic publications and channels
0.6	05/11/2020	Heini Jarvinen, TECH.EU	T5.1 Dissemination and MSE ecosystem-building, finalising and editing contributions
0.7	06/11/2020	Amedeo D’Arcangelo, KPS Samuel Fricker, FHNW	Introduction, contributions T5.2 Standardisation and liaison with policy
1.0	06/11/2020	Heini Jarvinen, TECH.EU	FINAL FIRST DRAFT VERSION FOR REVIEW
1.1	16/11/2020	Nuria Rodriguez, ATOS Jessica Peichl, PFH Bettina Schneider, FHNW Heini Jarvinen, TECH.EU	Review comments Additions to GEIGER education & introduction Additions to academic publications and channels Integrating review comments
1.2	17/11/2020	Samuel Fricker, FHNW	T5.2 Standardisation and liaison with policy
1.3	23/11/2020	Heini Jarvinen, TECH.EU	Integrating comments, editing
1.4	24/11/2020	David Elfassy, KPMG Lior Armive	Review comments on T5.2 Review comments on T5.1
1.5	24/11/2020	Samuel Fricker, FHNW	Integrating review comments T5.2
1.6	25/11/2020	Heini Jarvinen, TECH.EU	Integrating review comments T5.1, Summary and conclusions FINAL VERSION
1.7	25/11/2020	Natalie Jonkers, FHNW	Review, quality control and formatting
1.8	27/11/2020	Cristian Priboi, CERT-RO Dumitru David, CERT-RO Samuel Fricker, FHNW	Standards related to cybersecurity domain modelling
1.9	27/11/2020	Heini Jarvinen, TECH.EU	Introduction and Summary, quality control
2.0	30/11/2020	Samuel Fricker, FHNW Bettina Schneider, FHNW	Quality control and submission

Contents

Executive summary	xii
1 Introduction	1
2 T5.1 Dissemination and MSE ecosystem-building	6
2.1 Introduction	6
2.2 Impact goals	6
2.3 Approach and methodology - pathway to impact through communications and dissemination	9
2.4 Who: Target Audiences	11
2.4.1 Small businesses - the end user	12
2.4.2 Associations and networks for small businesses	12
2.4.3 Security Defenders (audiences for GEIGER education)	15
2.4.3.1 Service providers	16
2.4.3.2 MSE members-in-education	16
2.4.4 Communities with overlapping interests	16
2.4.5 Other target audiences	17
2.4.6 Priorities for engaging target audiences	18
2.5 What: Key messages	20
2.6 How: Tools, channels, activities, materials	22
2.6.1 Visual style	23
2.6.2 Website	23
2.6.3 Social media	24
2.6.4 Newsletter	25
2.6.5 Events	25
2.6.6 Mass media	27
2.6.7 Academic publications and channels	29
2.6.8 Promotional and information material	30
2.6.9 Overview of tools, channels, activities, and materials per target audience	31
2.6.10 Partners' roles	32
2.6.11 Internal organisation of dissemination and communications work	33
2.7 When: Timeline	34
2.7.1 Project launch & preparation phase (M1-M6)	35
2.7.2 GEIGER development and building education provider community (M7-M18)	35
2.7.3 GEIGER refinement (M19 - M24)	35
2.7.4 GEIGER rollout & release (M25-M30)	36

2.7.5	Post-project	36
2.8	Criteria for measuring success	36
2.9	Achievements to date	36
2.9.1	Logo and visual style	36
2.9.2	Website	38
2.9.3	Social media	39
2.9.4	Newsletter mailing list	40
2.9.5	Events	41
2.9.5.1	Kick-off	41
2.9.5.2	Pilot use case kick-off workshops	41
2.9.5.2.1	Swiss use case workshops	41
2.9.5.2.2	Romanian use case kick-off workshop	42
2.9.5.2.3	Dutch use case kick-off workshop	43
2.9.5.3	Cluj Innovation Days panel discussion	43
2.9.5.4	Participation in other events	45
2.9.6	Mass media	45
2.9.7	Promotional and information materials	45
2.9.7.1	Flyer	45
2.9.7.2	Roll-up	46
2.9.7.3	Branded giveaways	47
2.9.7.4	Partner publications	48
2.9.7.5	Connecting with multipliers	48
2.9.8	Overview of dissemination and communications activities	49
2.10	Impact tracking	50
2.10.1	Risk management	51
2.11	Summary and Conclusions	53
3	T5.2 Standardisation and Liaison with Policy	54
3.1	Introduction	54
3.2	Methodology	57
3.3	Organisations and Initiatives	58
3.3.1	Standardisation	58
3.3.2	Policy Definition	60
3.3.3	Related Projects	61
3.4	Standards, Regulations, and Recommendations	62
3.4.1	SMEs	62

3.4.2	Cybersecurity	63
3.4.3	Data Protection and Privacy	65
3.4.4	Data Exchange and Information Sharing	65
3.4.5	Education Standards and Offerings	66
3.5	Selection of Standards and Regulations for GEIGER	67
3.5.1	GEIGER Solution	67
3.5.2	GEIGER Ecosystem	69
3.6	Expected Contributions to Standards and Policy	70
3.6.1	C1: Security Defenders Curriculum	70
3.6.2	C2: Open Security Tools API	71
3.6.3	C3: Information Sharing and Analysis API	71
3.6.4	C4: Protection of MSEs whose Business depends on Social Networks and Cloud-based Services under non-European Ownership	72
3.7	Summary and Conclusions	74
4	T5.3 Exploitation planning	75
4.1	Introduction	75
4.2	Approach and methodology	75
4.2.1	Pathway to impact through exploitation planning	76
4.2.2	Criteria for measuring success	82
4.3	Achievements to date	83
4.3.1	INSPIRE	83
4.3.1.1	Innovation Readiness Assessment	84
4.3.1.2	The INSPIRE online challenges	85
4.3.1.3	Inventory of the tools proposed by INSPIRE platform	85
4.4	Impact Tracking	88
4.5	Summary and Conclusions	88
5	Conclusion	89

Abbreviations, participant short names and glossary

Abbreviations

API	Application programming interface
B2B	Business to business
B2C	Business to consumer
CERT	Computer emergency response(/readiness) team
CMS	Content management system
CSIRT	Computer security incident response team
CTA	Call to action
CyberKit4SME	Tools for cybersecurity and data protection risk awareness, monitoring, forecasting, and management in small businesses
CyberSec4Europe	Governance structures for a future European Cybersecurity Competence Network
DEIP	A platform to collect all innovations done by all partners and protect as proof of ownership the results using blockchain technology
DoA	Description of action
GA	Grant agreement
GDPR	General Data Protection Regulation
ECISO	European Cyber Security Organisation
EHR4CYBER	European Human Resources Network for Cyber
ENISA	The European Union Agency for Cybersecurity
ICT	Information and communications technology
INSPIRE	INtegrated Support of oPen Innovation pROfessionalization platform dedicated to assist SMEs for open innovations
IP	Intellectual property
IPR	Intellectual property rights
MISP	An open source threat intelligence platform and open standards for threat information sharing
MoUs	Memorandum of understanding
MSE	Micro and small enterprises
ME	Micro enterprise
MVP	Minimum viable product
MQ	Mapping questions
NGO	Non-governmental

NIS Directive	The EU Directive on security of network and information systems
OP	Operation principle
SDO	Standards-defining organisations
SME	Small and medium sized enterprise
SMESEC	A H2020 project to build a framework for protecting small and medium-sized enterprises
SRIA	Strategic Research and Innovation Agenda
TLR	Technology Readiness Level

Participant short names

FHNW	Fachhochschule Nordwestschweiz
UU	Universiteit Utrecht
TECH.EU	Fores Media Limited
KSP	Kaspersky Lab Italia Srl
PFH	Pädagogische Hochschule Freiburg
MI	Montimage EURL
KPMG	Somekh Chaikin Partnership
BBB	Berufsfachschule BBB Baden
ATOS	Atos IT Solutions and Services Iberia SL
SKV	Schweizerischer KMU Verband
HAAKO	Haako GMBH
CERT-RO	Centrul National de Raspuns la Incidente de Securitate Cibernetica
CLUJ IT	Asociatia Cluj IT
E-ABO	e-abo Gmbh
SCB	Braintronix Srl
PT	Public Tender Srl
SRA	Samenwerkende Registeraccountants en Accountants-Administratieconsulenten
CL	Coiffure Loredana

Glossary

“Baking” process	The process of mapping Markdowns to templates and building up all resources for the website
Beneficiary	Person or a group that derives benefit, profit, or advantage from the project

Communication	A strategically planned process that starts at the outset of the action and continues throughout the entire project, aiming at promoting the action and its results, and requiring strategic and targeted measures for communicating to a multitude of audiences, including media and the public, and possibly engaging in a two-way exchange
Dissemination	The public disclosure of the results by any appropriate means (other than resulting from protecting or exploiting the results), including by scientific publications in any medium
Lafley and Martin's Five-Step Strategy Model	A five-step model by A.G. Lafley and Roger Martin for developing a business strategy
Mendelow's power/interest matrix	A model for analysing the stakeholders of an organisation or a project that considers their power and likely interest to determine their potential influence
Markdown	A lightweight mark-up language with plain-text-formatting syntax, often used for formatting readme files, writing messages in online discussion forums, and to create rich text using a plain text editor
Multiplier	An organisation or individual who contributes to the promotion of and communications around the project towards its target audiences, amplifying the messages and bringing higher visibility to the project
Primary target audience	The segment or group of individuals or organisations that is most likely or desired to be the user of a particular product or service
Secondary target audience	The second most important segment or group to target the communications of a business or a project
Stakeholder	An individual, group, or organisation, who may affect, be affected by, or perceive itself to be affected by a decision, activity, or outcome of a project
Target audience	The intended audience or group of recipients for a particular message
Technology Readiness Levels	Indicators of the maturity level of technologies. This measurement system provides a common understanding of technology status and addresses the entire innovation chain. There are nine technology readiness levels; TRL 1 being the lowest and TRL 9 the highest.

List of tables

Table 1: Estimated significance of the GEIGER stakeholder groups for the European economy	5
Table 2: Key KPIs for T5.1.....	9
Table 3: Dissemination timeline, target audiences, messaging and blend of channels, tools and activities	11
Table 4: Key multiplier organisations that serve and connect with the MSE community.....	15
Table 5: Key target audiences, their interests and values, and barriers engage.....	22

Table 6: Potential international events to promote the GEIGER project.....	27
Table 7: Overview of tools, channels, activities and materials per target audience	32
Table 8: Dissemination and communication activities M1-M6.....	49
Table 9: Most likely risks related to the key KPIs of T5.1 and suggested actions to mitigate them...	53
Table 10: Key KPIs for T5.2	56
Table 11: Overview of the involved partners	57
Table 12: Requested inputs.....	58
Table 13: Relevance of the standardisation activities, and the involvement of GEIGER partners....	60
Table 14: Organisations influencing policy definition, their activities that are of relevance for GEIGER, and the GEIGER partners involved.....	61
Table 15: Projects related to GEIGER and GEIGER partners' involvement in them.....	62
Table 16: SME standards, regulations, and established recommendations of relevance for GEIGER	63
Table 17: Cybersecurity standards, regulations, and established recommendations of relevance for GEIGER.....	65
Table 18: Data protection and privacy standards, regulations, and established recommendations of relevance for GEIGER.....	65
Table 19: Data exchange and information sharing standards, regulations, and established recommendations of relevance for GEIGER.....	66
Table 20: Education standards, regulations, and established recommendations of relevance for GEIGER.....	67
Table 21: Coiffure Loredana's use of social networks and foreign cloud services.....	73
Table 22: Lean start-up flow	78
Table 23: Elements of the exploitation plan.....	82
Table 24: Potentially useful tools for the GEIGER exploitation plan.....	87

List of figures

Figure 1: Value of tooling for incident avoidance, detection, and mitigation (Ponemon 2018)	1
Figure 2: The three-step approach to impact.....	3
Figure 3: Target audience and multipliers.....	18
Figure 4: Level of stakeholder engagement, Mendelow's power/interest matrix.....	19
Figure 5: GEIGER project website, frontpage.....	24
Figure 6: Some of the GEIGER logo options presented during the design process	37
Figure 7: GEIGER logo	37
Figure 8: Example of a news markdown header and the corresponding groovy template	39

Figure 9: GEIGER social media campaign on the occasion of the European Cyber Security Month	40
Figure 10: GEIGER virtual kick-off and announcement of the project launch in Twitter	41
Figure 11: Swiss pilot use case workshop, the first in the series of the three GEIGER pilot kick-offs	42
Figure 12: Workshop in August 2020 to discuss how cybersecurity could be made more accessible to entrepreneurs running yoga studios	42
Figure 13: Romanian pilot use case workshop, organised as a hybrid event	43
Figure 14: Dutch pilot use case workshop, organised entirely online.....	43
Figure 15: GEIGER panel and virtual expo booth at the Cluj Innovation Days.....	44
Figure 16: GEIGER team at the RE Cares Requirements Engineering conference.....	45
Figure 17: Draft of the GEIGER introduction flyer	46
Figure 18: GEIGER roll-up	47
Figure 19: GEIGER listing on the Cyberwatching.eu Project Hub	49
Figure 20: The Cluj Innovation Days panel discussion around GEIGER and the digital resilience of small businesses was listed on the website of the European Cyber Security Month	49
Figure 21: Position existing maps and landscapes	54
Figure 22: The three life cycles	76
Figure 23: Combinations of the three life cycles.....	77
Figure 24: Possible combinations of the life cycle stages.....	77
Figure 25: Technology Readiness Level (TRL) and correlation with the GEIGER innovation process	79
Figure 26: Disruptive innovation strategy for the GEIGER solution	79
Figure 27: GEIGER must be directed for the creation of a fundamentally new product.....	80
Figure 28: INSPIRE Canvas.....	84
Figure 29: The six pathways of the CHALLENGES part of the INSPIRE online platform.....	85
Figure 30: DEIP Platform	88

Executive summary

To reach the maximum impact, the GEIGER project will adopt a multidimensional strategy for its dissemination, exploitation, and standardisation activities. It will focus on:

1. building the communities around the solutions to the challenges that small business experience in the field of data protection, privacy, and security risks, and facilitating a low-threshold adoption of the tools to address of these challenges,
2. harmonising the GEIGER technical framework and an education programme with third parties through standardisation,
3. contributing to the policy development with recommendations and dialogue,
4. assuring the full exploitation of the project results by, at the end of the project, creating the GEIGER organisation, a novel SME as an exploitation entity.

GEIGER dissemination and communication aims at raising awareness and interest towards the project among stakeholders, potential customers, interested communities, and all other relevant audience groups for the adoption of the project results. The primary target audience are small businesses, and the secondary target audiences are any groups and individuals that have potential to help us reach our primary target audience. We also aim at indirectly reaching out to our primary target audience through "Security Defenders", individuals who will have completed GEIGER education or training, and who can bring their expertise to micro- and small enterprises (MSEs) in or with which they work. The strategy will be based on major dissemination and communication channels and be designed as a blend of activities taking into account the respective target groups to be addressed. The GEIGER dissemination and communication strategy addresses a range of European, operationally diverse audiences, and relies on collaboration with multipliers and use of mass media. It includes, among other potential activities, communications through the GEIGER website, social media channels and newsletter, visibility in mass media and targeted media, academic publications, and organisation of and participation in events and workshops. The existing channels, tools, and contacts of the consortium partners are its backbone, and they will be used to reach the local audiences, in particular in the pilot use case countries. The channels and tools being used vary from one consortium partner to another, and the dissemination and communication strategy aims at guaranteeing the efficient use of these resources, and thus maximising the impact of the project.

The GEIGER Solution will consist of the technical framework and the Security Defenders education that is open to related activities within Europe and worldwide offering maximal cybersecurity and data protection impact for micro and small enterprises (MSEs). Such openness can only be achieved through harmonisation and mutual recognition of external interfaces with third parties, which can be enabled with standardisation. Lessons-learned from testing, validating, and demonstrating the implementation are intended to be shared back to the organisations that define and maintain the respective standards. If no suitable standard can be identified but a harmonised definition of the interface is necessary for the openness of the ecosystem, GEIGER will initiate a dialogue with relevant stakeholders to enable standardisation.

The project will also contribute to policy development at national and European level, with recommendations and dialogue, drawing on the lessons learned from the piloting with MSEs, SME associations, and CERTs/CSIRTs. The aim is to support the dialogue on national and/or European legislation.

To guarantee the continuation of the tools and the ecosystem built during the project, the GEIGER project will initiate an organisation, a start-up company, for managing and evolving the GEIGER Framework for joint exploitation. The GEIGER consortium will prepare the jointly developed

innovation for sustainable rollout across Europe. The GEIGER organisation will provide the opportunity for open governance of the GEIGER Solution by firms such as established SME associations, educators, and CERTs that can offer needed market and industry knowledge, a factor critical for the success or failure of any platform.

1 Introduction

This document presents the preliminary stakeholder and impact analysis, and the initial dissemination and communication, standardisation, and exploitation strategies for the GEIGER project. These strategies will be continuously evaluated and adjusted along the duration of the project, to maximise the project's impact. The document also lists the key achievements for the WP5 work during the period of M1-M6 of the project.

GEIGER recognises the vital role that small businesses play in reducing damage due to data-related incidents for the European economy. SMEs constitute the majority of the players in the EU economy and, are more vulnerable than the large players due to lack of awareness and of skills to use suitable tools to prevent digital security incidents. The key challenges of the small businesses are problems in hiring skilled workers, making it difficult to access security, privacy, and data protection knowledge, and limited access to finance, making investment in tools, infrastructure, and processes difficult. This limits the small businesses' capacity to grow and compete.

The economic damage of data breaches is significant for each MSE and, consequently, for the whole European economy. According to Ponemon Institute LLC, the average cost of a data breach is 3.5€ million with an average cost per record of 130€. The likelihood that an organisation will have one or more data breaches over a duration of two years is estimated by 28% on average. According to these figures, a concerted attack may damage many of the more than 23 million European small businesses or even put them out of business, severely damaging the European economy.

According to the same study, tools can reduce the cost of incidents by up to 84% through the automation they provide for incident avoidance, detection, and mitigation. The mean time to identify a breach was 197 days, and to contain it 69 days. Improved incident detection and resolution times were associated with 35% reduced incident costs. The availability of skills and tools can reduce the likelihood of incidents in MSEs by ensuring that best practices are in place, relevant tools are adequately used, and a culture is established that safeguards data in the company. 27% of the incidents are caused by human error, 48% by malicious attacks.

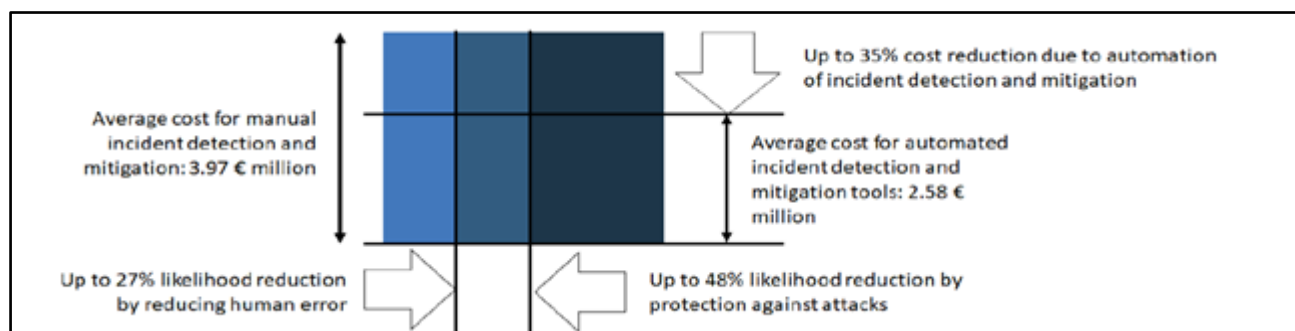


Figure 1: Value of tooling for incident avoidance, detection, and mitigation (Ponemon 2018)

Taking into account these contextual factors, GEIGER will contribute in the following:

Boosting European SMEs&MEs' competitiveness: Increased trustworthiness of MSEs through security and compliance will promote their growth. To compete with the US and Asian market, the inclusion of security within the MSEs structure is a fundamental pillar for providing efficient and reliable services and products for our society. In this context, GEIGER proposes radical changes via an innovative security solution that will connect small businesses with competent players through multiple channels: towards CERTs/CSIRTs through incident reporting and recommendations, towards educational and service providers through Certified Security Defenders, towards tool

providers through the GEIGER toolbox. These connections will allow MSEs to reduce capital investment in monitoring, forecasting and assessing security, privacy, and data protection threats. GEIGER will thus have a significant effect on the competitiveness of European small businesses in the field of digital solutions. Finally, security-related concerns and barriers that currently prevent exploitation of new business opportunities will be lowered and hence boost European entrepreneurship.

Positioning Europe as the “centre of gravity” for security solutions: GEIGER builds on existing best-effort security products, enriches them with novel solutions (such as the GEIGER Indicator and Security Defenders education) and positions highly reliable and cost-effective European security solutions worldwide. Thus, GEIGER will contribute to putting Europe in a unique position and fosters European competitiveness in providing technologies for industrial and digital networks.

Expected impact:

Economic damage caused by harmful cyber attacks, privacy incidents and data protection breaches is reduced, and GEIGER will pave the way for a trustworthy EU digital environment benefitting all economic and social actors.

The project will follow the three-step approach illustrated in the figure below for generating the expected impacts:

Step 1: GEIGER will develop experiential challenge-based education of security, privacy, and data protection skills for Security Defenders available to small businesses. We will also create an extensible GEIGER Toolbox for incident avoidance, detection, and mitigation in MSEs, and a GEIGER Cloud in which the GEIGER Indicator and an incident database are running and connecting the framework of MSEs, SME associations, CERTs/CSIRTs, Security Defenders, and relevant third-party actors.

Step 2: The resulting GEIGER Framework is then piloted for evaluating the socio-technical alignment and impact of the GEIGER Framework and GEIGER Education Ecosystem in concrete diverse use cases at TRL7.

Step 3: An organisation is created for rolling the GEIGER Solution out and creating Europe-wide impact with a sustainable business model and based on the lessons learned during the GEIGER project.

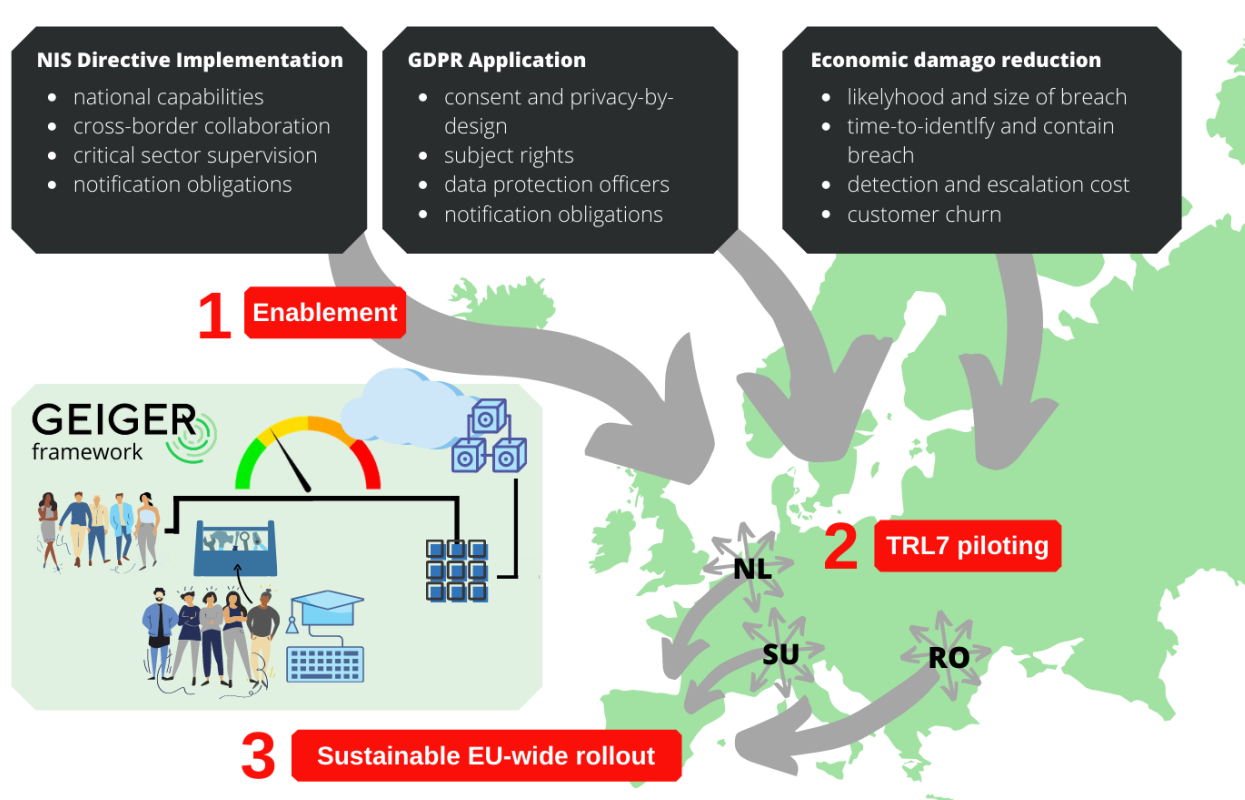


Figure 2: The three-step approach to impact

WP5 of the project, Dissemination and Exploitation, aims at achieving widespread awareness, interest, and support for the GEIGER solution by bringing the following stakeholders into the GEIGER ecosystem: SMEs with a focus on micro and small enterprises (MSEs), education, tool developers and service providers like cyber ranges, CERTs, and security experts. The following table shows the significance of each stakeholder group for the European economy and reflects the massive opportunity that GEIGER can produce in better protecting these MSEs thanks to contributing to the implementation of the Directive on security of network and information systems (NIS Directive) and the application of the General Data Protection Regulation (GDPR).

Stakeholder	Characterisation	Significance for the EU
MSEs	Most MSEs do not consider security and data privacy as a priority but are at risk increasingly. Many are occupied with day-to-day business and have no expertise in data protection and cybersecurity.	24.5 million SMEs representing 99% of the players in the EU economy ¹ . 2 700 000 enterprises were newly born in 2017 ² .

¹ <https://www.statista.com/statistics/878412/number-of-smes-in-europe-by-size/>

² https://ec.europa.eu/eurostat/statistics-explained/index.php/Business_demography_statistics#Active_enterprises_in_the_business_economy

Education providers	Education providers such as vocational schools or MSE associations offer target-group specific training on a specific set of subjects. In general, they hold long-term and trustworthy relations to MSEs, as well as their apprentices.	In Germany, Austria, Slovakia, Denmark, and Ireland, apprentices make up 2.5%-5.3% of the staff in firms ³ . Also in Switzerland, two thirds of the adolescents make the decision for vocational training as apprentices ⁴ .
Adult learners	Adult learners are interested in gaining knowledge and develop personal skills necessary within their own personal life or workplace.	In 2016, 44.4% of people in the EU aged 25 to 64 took part in education and training, the majority of which participating in non-formal education and training. In 2016, employers in the EU were the most common providers of non-formal education and training activities (33.8%).
Tool developers and service providers	Cybersecurity tool developers and service providers aim for defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks through their products and services. Advanced solutions for SMEs are available in the EU market to protect sensitive business data, allowing for example to detect and patch vulnerabilities for reducing attack entry-points and to encrypt data for preventing data leaks.	Hundreds of cybersecurity tool developers and service providers enterprises are established in the EU, more than 50 of which are located in France and around 70 of which are based in Germany, Austria or Switzerland in 2020.
CERTs	CERTS, such as the Swiss National Cyber Security Center (NCSC), provide up-to-date and relevant data on current cyber threats that have been reported. Considering the information collected and provided by CERTs helps to prioritise the threats that will be approached within several aspects of GEIGER.	About 400 CERTs/CSIRTs are established in Europe ⁵ .

³ <https://www.cedefop.europa.eu/en/publications-and-resources/statistics-and-indicators/statistics-and-graphs/bridging-learning-and>

⁴ http://www.berufsbildung.ch/dyn/bin/2777-13558-1-fakten_zahlen_bb2019_dt.pdf

⁵ <http://www.enisa.europa.eu/topics/csirts-in-europe/csirt-inventory/certs-by-country-interactive-map>

Security experts	The security experts are responsible for providing security during the development stages of software systems, networks and data centres; they are able to identify vulnerabilities and risks in hardware and software, and to manage and monitor attacks and intrusions, suggesting security measures for any information and designing strategies and defensive systems against intruders.	Hundreds of thousands of workers in the EU own the Security experts skills, 121.000 of which working in France and 133.000 of which working in Germany in 2019. However, the actual requirement for such professionals is much higher; in fact, the EU labour market has hit a shortage of over 200.000 Security experts.
------------------	--	---

Table 1: Estimated significance of the GEIGER stakeholder groups for the European economy

The mobilisation of these stakeholders is challenging. In a recent expert workshop on skills for SMEs hosted by the European Digital SME Alliance, the conclusion was reached that today, no systematic approach is known to reach all of the 24'500'000 SMEs&MEs in Europe for raising awareness and bringing the skills and tools needed to allow them to become active players and achieve resilience and compliance. In particular, the experts noted that social media campaigns were ineffective in reaching small businesses with the security, privacy, and data protection topics.

GEIGER will address the mobilisation challenge by leveraging existing networks like SME and professional associations, value chains as established by educators for young employees, start-up ecosystems, and accountancy service providers, and by cooperating with mass media. WP5 also aims at coordinating a European MSEs risk reduction roadmap with CERTs/CSIRTs, SME associations, and educational stakeholders in joint events, and standard and policy defining activities, including a final conference for initiating EU-wide roll-out of GEIGER. WP5 finally aims at refining and testing the business model in close collaboration with the use case pilots (WP4) and preparing the GEIGER organisation needed to sustainably operate GEIGER according to the European risk reduction roadmap.

The remainder of this document is structured as follows. **Chapter 2, T5.1 Dissemination and MSE ecosystem-building**, describes the goals of the GEIGER dissemination and communication, its target audiences, key messages, tools, channels, activities and materials, and the initial strategy and timeline for actions, and presents the methods of tracking the progress and mitigating risks related to different areas of the strategy. It also describes the dissemination and communication results achieved during the M1-M6 of the project. **Chapter 3, T5.2 Standardisation and Liaison with Policy**, describes existing standardisation and planned contributions to standards and policy. **Chapter 4, T5.3 Exploitation planning**, presents the initial implementation strategy for rolling out GEIGER. **Chapter 5, Conclusion**, summarises and concludes.

2 T5.1 Dissemination and MSE ecosystem-building

2.1 Introduction

The aim of the dissemination and communications plan is to raise awareness and interest towards the project among stakeholders, potential customers, interested communities, and all other relevant audience groups for the adoption of the project results. The plan will be based on major dissemination and communications channels, and be designed as a blend of dissemination activities taking into account the respective target groups to be addressed.

Every project partner will ensure that dissemination activities are to be carried out nationally, and if applicable, will contribute to disseminate the project's results internationally. As such, dissemination aims at generating values for EU industries and academia. As soon as the first exploitable deliverables are generated, the project partners will disseminate the project's results to both scientific and industrial communities and other target groups in the EU, in order to stimulate awareness. The dissemination content should prepare and convince the audience for the benefits of the (expected) project outcomes.

The dissemination and communications goals are aligned to the overall project aims are: a) maximise our reach to **micro and small enterprises (MSEs)** as well as associations and networks representing them, in order to convert them to users, b) maximise our reach to education providers and institutions in order to secure their commitment to add the Security Defenders education to their offering, and c) establish a framework and secure partner commitment for Europe-wide roll-out and sustainable exploitation after the project period, demonstrated through the incorporation of the tool and other project outcomes into their offerings.

The communications strategy addresses a range of European and international (e.g. Israeli, reflecting the range of consortium partners), operationally diverse audiences and relies on collaboration with multipliers and use of mass media. This context drives both challenges and the opportunities. We will establish a clear message based on the GEIGER risk indicator and focus on mass media to win MSEs as potential users and start already early in building collaborative relationships with important stakeholder groups, including CERTs/CSIRTs, existing education providers, and association and networks for small businesses. By utilising mass media and activating European and national organisations, we will reduce our points of contact and create a cascade approach with trusted sources, to reach more MSEs.

2.2 Impact goals

T5.1 implements the dissemination work, aiming at awareness of the GEIGER challenge and project, raising interest in the GEIGER solution and ecosystem, and stimulating the desire to adopt GEIGER. Tech.eu leads the consortium in this task. KPIs are analysed and the impact of dissemination activities evaluated throughout the duration of the task to initiate corrective action early if necessary.

The following table lists the key KPIs for T5.1. The table gives a high-level overview of the tools to be used to reach the KPIs, the timing in relation to the different stages of the project, and the most relevant target audiences. The communication tools and actions will be tailored to correspond to the needs of each geographic/demographic target audience, in collaboration with the partners with local and field-specific expertise.

KPI	Description of objectives	Timing / stage of the project	Target audience(s)	Tools and actions to reach the KPI
I2.1.4.1	IMPRESSIONS ≥1'000'000 impressions of the GEIGER Indicator as measured by number of impressions of media channels	M1-M30	MSEs, all stakeholders	<ul style="list-style-type: none"> • Mass media visibility through actions coordinated among consortium members • Targeted media (e.g. trade magazines) visibility through collaboration with multipliers • Social media actions and collaboration with multipliers • Event organising and collaboration • Website articles (GEIGER and partners, including Tech.eu)
I2.1.1.1	ATTENTION >500'000 SMEs&MEs will be aware of the GEIGER Indicator as a dynamic risk monitoring instrument	M7-M30	MSEs	<ul style="list-style-type: none"> • Brand awareness through consistent and recognisable messaging and style of communications, including relatable and emotionally appealing storytelling • Creation of newsletter mailing list and campaigns to encourage subscriptions • Social media actions and campaigns encouraging to engagement • Organisation of and participation in events and workshops
I2.1.2.4	INTEREST > DESIRE ≥100'000 small enterprises have a GEIGER account, allowing them to predict their risk with the personalised GEIGER Indicator and benefit from the GEIGER toolbox.	M25-M30	MSEs	<p>Raising further interest, education on cybersecurity issues, and encouraging to test the GEIGER toolbox by:</p> <ul style="list-style-type: none"> • Communications sent via the newsletter mailing list • Mass media visibility • Targeted media visibility • Organising/facilitating workshops/webinars

I2.1.4.3	INTEREST > DESIRE ≥20 SME associations or chambers of commerce in ≥50% of the member states will have confirmed their intent to recommend the GEIGER Framework among their member enterprises.	M19-M30	SME associations / chambers of commerce	<ul style="list-style-type: none"> • Awareness-raising (on both GEIGER toolbox and possibilities of offering GEIGER education) and networking through participation in events and targeted publications, coordinated with consortium members with connections to SME associations and chambers of commerce
I2.1.4.4 I2.1.1.7 I2.1.1.6 I2.1.1.8	INTEREST > DESIRE ≥50 education providers, incl. schools/ universities, professional associations or unions, and incubators or accelerators for start-ups, will have confirmed their intent to offer the GEIGER education.	M19-M30	Education providers, industry clusters, incubators, accelerators, MSE associations, chambers of commerce	<ul style="list-style-type: none"> • Awareness-raising and networking through participation in events and targeted publications, coordinated with consortium members with connections to education providers
I2.1.4.5	INTEREST > DESIRE ≥50% of the CERTs/CSIRTs in member states will have confirmed their intent to interoperate with the GEIGER Framework.	M19-M30	CERTs/CSIRTs	<ul style="list-style-type: none"> • Awareness-raising and networking through participation in events and targeted publications, coordinated with consortium members with connections to CERTs/CSIRTs

I2.1.1.2	ACTION - Adopt toolbox >50'000 SMEs&MEs will have tried the personalised GEIGER Indicator for their own specific SME&ME by registering on GEIGER Solution	M25-M30	MSEs	Encouraging the installation and adoption of the GEIGER toolbox via: <ul style="list-style-type: none"> ● Communications sent via the newsletter mailing list ● Mass media visibility ● Targeted media visibility ● Organising/facilitating workshops/webinars ● Activating trusted advisors, associations and networks through resources pack
----------	---	---------	------	---

Table 2: Key KPIs for T5.1

2.3 Approach and methodology - pathway to impact through communications and dissemination

The objectives of the dissemination and communication of the GEIGER project are to first build awareness around the project and the value it could add to different stakeholders, and to generate interest among those stakeholders. The goal of the dissemination actions is to efficiently disclose the project results within the academic community, using scientific publications and events as the principal channel. The communication actions aim at raising awareness on the project itself and its results among the general public (including through media), prioritising the selected key target audiences, through strategic and targeted measures, and engaging in a two-way exchange with them.

Once the desired target audiences have been reached, and they have developed an interest towards GEIGER, the next objective is to incite action - registering their interest, for example in a form of subscription to our further communications, and in the case of our primary audience, MSEs, the installation and testing of the GEIGER toolbox, and in the case of our secondary target audiences, an indication of an intent to recommend or use the GEIGER Solution, or to include it in their offerings. Lastly, the dissemination and communication of the project aims at supporting the sustainable exploitation of the project result and the launch of the spin-off organisation at the end of the project lifetime.

To build the basis of the dissemination and communication strategy for the GEIGER project, we used the 'Five Ws and How' (5W1H) approach to analyse all its aspects. This tool is most known for its use by journalists, but also proven beneficial when applied to project management and communications.

The 5W1H approach allows us to determine the action plan that should be put in place. First, it helps us understand and define **who** our audiences - those potentially impacted by the project, those taking action, and those supporting us - are, and what are their values and preferences. This is critical for succeeding to relay our message. Secondly, it allows us to consider **what** our target audiences need or want from us - **why** would they engage with us - and what are their interests and values linked to the GEIGER project. Based on this, we will be able to define the framing and the key messages we wish to communicate. Finally, the 5W1H approach helps us build the detailed strategy for **how** we intend to proceed to reach the desired impact and results indicated in our KPIs, as well as its timeline (**when**), including the events and occasions **where** we see potential for communicating and raising awareness on the project.

The table below gives an overview of the dissemination and communications objectives, key messages, target audiences, focus channels and the most relevant materials and actions for each stage of the project.

	M1 - M6	M7 - M18	M19 - M24	M25 - M30	Post-project
Stage of GEIGER project	Project launch & preparation phase	GEIGER MVP development	GEIGER MVP refinement	GEIGER MVP rollout & release	Exploitation
		Education Provider community	Security defenders community		
Dissemination Objective	Awareness building	Generating interest	Register	Install (letters of intent)	Sustainability
Dissemination and communications strategy					
Goals	Internal alignment: Initiating contacts and awareness on the project	Building communities: Education providers and SME associations/ networks	Coordinating actions with multipliers to reach and activate our primary audience	Introducing the GEIGER toolbox (beta version) and activating MSEs to install and test it	Facilitate a successful roll-out of the GEIGER spin-off to bring a finalised solution to MSEs
Key messages	Introducing project, highlighting cybersecurity challenges and GEIGER's role in overcoming them	Acknowledging the typical cybersecurity challenges, emphasising the potential benefits of GEIGER to MSE & education provider communities	Encouraging to test the cybersecurity practices of your MSE, evaluate level of risks, and sign up for testing GEIGER	Explaining the practical functionalities of GEIGER toolbox and its benefits for the user	TBD
Key target audiences	Consortium members, their existing contacts, potential multipliers	Education providers, SME associations and networks	SME associations and networks, MSEs, education providers, Security Defenders community	MSEs, Security Defenders community	MSEs, Security Defenders community

Focus channels	Setting up all channels, mass media	Event participation, newsletter, direct contacts and networking, mass media, targeted publications	Targeted publications, mass media, event participation/organisation, newsletter	Mass media, targeted publications, event participation/Organisation (incl. final workshop), newsletter	TBD
	GEIGER website and social media channels, partner channels, Tech.eu channels				
Materials and actions	Collection of use case material, articles, flyer, roll-up, giveaways, event participation, panel discussion	Visual and audio-visual material, panel discussions, newsletter updates	Op-eds / opinion pieces, targeted workshops, webinars, newsletter updates	Op-eds / opinion pieces, panel discussions, keynotes, practical workshops, project's final workshop, webinars, newsletter calls-for-action	TBD
		High impact stories, interviews			
	Press releases and briefings, social media contents, web articles / blogs, event participation and organising, scientific publications				

Table 3: Dissemination timeline, target audiences, messaging and blend of channels, tools and activities

2.4 Who: Target Audiences

Dissemination and communication will support the ambitious goal of the GEIGER project to reach out to all key stakeholders connecting small businesses and to the cybersecurity community, and to bring them together.

The GEIGER project will enter in dialogue with CERTs/CSIRTs and larger providers for security and data privacy technology for standardisation of notification and information data exchange as well as with existing educators for the positioning and definition of the Security Defender education and certification. The project will also aim at building an education provider community for the sustainable development and maintenance of the education tools, as well as the Security Defenders community, which guarantees the sustainable existence and growth of trained and apprentice Security Defenders.

The dissemination and communications strategy will target all directly involved and interested stakeholders. The stakeholders in the GEIGER Ecosystem are thoroughly introduced in D1.1 Requirements. These target audiences include as **primary target audience small businesses**, and as **secondary target audiences any groups and individuals that have potential to help us reach**

our primary target audience, such as SME associations and networks, communities and projects with overlapping interests, and public institutions and initiatives for small businesses.

In addition to this, we aim at indirectly reaching out to our primary target audience through individuals who will have completed the Digital Security Defenders education and can bring their expertise and the GEIGER tools to MSEs in or with which they will be working. In this sense, it is important to list as our target audiences also education and training providers, who could potentially include the GEIGER Security Defenders programme to their curricula or training offering, and thus help building the Security Defender community.

2.4.1 Small businesses - the end user

The primary targets for our dissemination and communications strategy are **MSEs within Europe**, as they will be the end users for the GEIGER tool. These enterprises make up the overwhelming percentage of non-financial enterprises in Europe. As identified earlier in the report, there are 24.5 million SME in the EU 28 and of these 93% are MSE. Although they can be neatly packaged under the title of MSEs, in reality, they are a hugely diverse group that ranges from traditional, well established local family businesses to young newly formed tech start-ups, and everything in-between.

Given the nature and networked characteristic of the primary audience we also need to address the secondary target audience, those who influence, advise, and support the primary target audience. This secondary target audience is even more diverse than the primary audience, spanning service providers of all sizes and governments with their agencies.

2.4.2 Associations and networks for small businesses

Associations, chambers of commerce, and clusters offering small businesses and start-ups advice, a community, and a voice in the legal dialogue will constitute an important multiplier for the communications efforts of the project, and play a crucial role in building the GEIGER ecosystem and amplifying the impact of the GEIGER project. We will reach out to professional associations (vertical), SME associations (horizontal), and umbrella organisations of these associations. For the successful communications of the project, and to build the desired impact, it is critical to build relations to and to work closely with these associations and networks, and to exploit to the maximum the existing channels they possess to reach their audiences.

In the Swiss pilot use case, the involved SME association SKV, with 1000 active member SMEs&MEs (in 2019), will help us connect with the local businesses, and in building appealing messaging around GEIGER. In the Romanian use case, ClujIT, founder and coordinator of a network of IT clusters from Balkan, Black Sea and Baltic countries (20+ clusters), will pilot GEIGER for diffusing good practice in security, privacy, and data protection through the simple and relevant awareness message and low-threshold adoption of the GEIGER toolbox, supported by the Security Defenders. ClujIT incorporates more than 80 software companies, eight universities and ten catalyst organisations, including accelerators and digital innovation hubs. In the Dutch use case, SRA who unite 375 SME audit accountancy and tax advisory firms, will contribute to raising awareness of the GEIGER solution among the accountants within its membership. Their affiliated firms serve around 55% of Dutch SMEs. Beyond the project consortium partners, we have identified other key multiplier organisations that serve and connect with the MSE community. Some of these are illustrated below:

Organisation	Focus	Countries	Mission	Membership
EEN-Enterprise Europe Network	SMEs	Europe	EEN helps businesses innovate and grow on an international scale. It is the world's largest support network for SMEs with international ambitions.	600+ affiliated organisations in 60 countries
European Digital SME alliance	SMEs	Europe	European association of SME/MEs in the ICT sector	30 regional/national SME organisations representing 20 000 digital SMEs
European Startup Network	Start-ups and digital MSEs	Europe	ESN unifies national start-up associations to create a common voice for European start-ups so that more can start, scale, and succeed in the EU.	24 affiliated organisations and a network of 30 000+ start-ups
Startup Europe Club	Start-ups and digital MSEs	Europe	The Startup Europe Club, for start-ups to find everything they need in one place.	615 start-ups
SMEunited	SMEs	Europe	SMEunited, formerly known as UEAPME, is the association of crafts and SMEs in Europe, representing national cross-sectoral Craft and SME federations, European SME branch organisations and associate members.	24 million SMEs in Europe which employ almost 95 million people
Eurochambres	SMEs	Europe	Eurochambres represents an umbrella organisation with over 45 members (43 national associations of chambers of commerce and industry and two transnational chamber organisations) and a European network of 1700 regional and local chambers.)	Over 20 million businesses more than 93% are SMEs

Accountancy Europe	Accountants	Europe	Unites 51 professional organisations from 35 countries that represent 1 million qualified accountants, auditors and advisors	51 professional organisations representing 1 million accountants
Schweizer Unternehmen für Prüfung, Treuhand, Steuern und Beratung (BDO)	SMEs	Switzerland	BDO is an independent Swiss firm operating in the auditing, accounting, tax and consulting services arena.	23 377 clients (2019)
Schweizerischer Gewerbeverband sgV / l'Union suisse des arts et métiers usam	SMEs	Switzerland	A Swiss umbrella organisation for SMEs in the field of arts and crafts.	Represents 230 associations and some 500,000 companies
ICTswitzerland	Large and medium sized enterprises (ICT)	Switzerland	ICTswitzerland is the umbrella organisation for the digital economy. It promotes digital technologies as well as the education and further training of ICT specialists and is committed to the identification and prevention of cyber risks.	Brings together 34 large and medium enterprises, along with 21 associations
swissICT	Businesses of all sizes	Switzerland	swissICT is the largest professional association in the ICT industry and is the only association that connects ICT providers, users and specialists in Switzerland.	Over 2500 members
Chamber of Commerce and Industry of Switzerland (SIHK/CCIS)	Businesses of all sizes	Switzerland	CCIS promotes the exchange of knowledge and experiences between the cantonal CCIs, represents the political and economic interests of the CCIs within economiesuisse, jointly develops and promotes services, and represents the CCIs in European committees.	The union of the 19 cantonal and regional chambers of commerce in Switzerland and the Liechtenstein Chamber of Commerce

Association of Owners and Handcrafts	Businesses of all sizes	Romania	An employers' association in Cluj-Napoca region, a founding member of CNIPMMR.	(Unknown)
The National Council of Small and Medium Private Enterprises in Romania (CNIPMMR)	SMEs	Romania	CNIPMMR is an employers' confederation that ensures the unitary representation of the interests of SMEs and of the employers' movement of SMEs at national and international level.	8 regional federations and 98 affiliated members
The Netherlands Chamber of Commerce	Businesses of all sizes	The Netherlands	Netherlands Chamber of Commerce officially registers companies and gives them advice and support.	(Unknown)
NBA - The Royal Netherland Institute of chartered accountants	Accountants	The Netherlands	The professional body for accountants in the Netherlands	+1000 affiliated organisations and over 21,000 members

Table 4: Key multiplier organisations that serve and connect with the MSE community

GEIGER will refine and test the impact of awareness-creation and skill development in collaboration with these SME associations and networks involved or associated with the GEIGER project. Surveys will be issued to the SME associations' members to test the MSEs awareness of the GEIGER Indicator and access to the GEIGER tools and Certified Security Defender skills.

Typically, these associations organise several events every year, giving the opportunity to meet and discuss GEIGER with their members, and GEIGER aims at being present at these events for assessing and evolving the capacity-building strategy.

2.4.3 Security Defenders (audiences for GEIGER education)

In addition to reaching out to MSEs directly with the intention to introduce the GEIGER solution, the project aims at connecting with them also through the "Cyber Security Defenders". We will target our communications towards education providers who could potentially include the GEIGER Security Defenders programme to their programme, to build the GEIGER education providers community and education ecosystem.

The **education providers** in this target audience include, among others, vocational schools (such as BBB in the Swiss pilot use case), associations offering training to service providers for SMEs (such as SRA in the Dutch pilot use case), and networks and clusters offering training to entrepreneurs and small businesses (such as ClujIT in the Romanian pilot use case), including training providers for adult education.

Within the project and especially after the project lifetime, a community of Security Defenders will ensure an exchange network of the Security Defenders that can be seen as an added value to the Security Defender Education. Likewise, a community of education providers will be set up with its

main tasks in coordinating the general education and keeping the training up to date in content and format.

In the follow-up of the project, the Security Defender Education, particularly for the 'Certified Security Defender' will be exploited by setting competence standards that can be applied in an international framework.

2.4.3.1 Service providers

We will address entities of individuals providing services to MSEs, such as accountancy, legal advice, and ICT services, as one of our most important secondary audiences. These service providers allow MSEs to outsource certain business operations, and hence offer an entry point to reaching them with security, privacy, and data protection issues. They will be able to approach small businesses and to introduce GEIGER toolbox to them by exploiting their Security Defenders education as a diversified business offering (e.g. provided by accountants and ICT services) or as a start-up business (e.g. developed by entrepreneurs).

As in the case of small businesses, the most efficient way to reach these service providers is through their associations and networks. They allow connecting with our actual secondary target audience, service providers, via already established and trusted channels.

In the Netherlands, the accountant association SRA will be playing an active role in the project and leading the Dutch use case. However we will also establish links with [NBA - The Royal Netherland Institute of chartered accountants](#) who have +1000 affiliated organisations and over 21,000 members, and similar organisations such as [Accountancy Europe](#) who represent over 1,000,000 accountants in 35 countries.

2.4.3.2 MSE members-in-education

MSE members-in-education such as apprentices will, similarly to service providers, offer a natural entry point to connect with MSEs regarding their cybersecurity. During their studies, the future apprentices will complete the Security Defenders education programme, and when moving on to work as an apprentice, often in an MSE, they will be able to bring security, privacy, and data protection experiences sustainably to these small businesses, which will increase their self-efficacy.

These MSE members-in-education will be mainly targeted through their education providers. Targeting existing education offerings for dissemination is a unique and thus far little tried mechanism for reaching MSEs.

In the Swiss use case pilot, Berufsfachschule BBB will offer the Security Defenders programme to their vocational school students. In the Romanian pilot, ClujIT will offer the cybersecurity training to entrepreneurs in their network, and in the Dutch pilot, SRA will add Security Defender modules to their training offering.

2.4.4 Communities with overlapping interests

In addition to relying on the SME associations and networks for supporting our dissemination efforts, reaching out directly to other multipliers to raise awareness of the existence of GEIGER project and toolbox will increase the impact of our communications. Any organisation or community with overlapping interests, such as educating their audiences on cybersecurity issues, or providing services to small businesses, is a potential multiplier for the dissemination of the GEIGER project.

Examples from our landscape mapping are [European Union Agency for Cyber Security](#) (ENISA) or [Digital Trust Center](#) in the Netherlands, with a membership of over 1000 companies. There are also EU funded initiatives such as [Cyberwatching.eu](#) and [Cyberwiser.eu](#) as well as private counterparts such as [The European Cyber Security Organisation](#), [Women4Cyber Registry](#) and [Global Cyber Alliance \(GCA\)](#). These organisations and communities will also include other EU projects dealing

with similar topics, “cyber community”, NGOs (such as privacy advocates or those providing services to MSEs), European associations participating in the legislative process and connecting national and local associations, other European initiatives to enhance the required unity of the European research task force and increase the innovation impact in the area, or the scientific and research communities focusing on the innovation and technological aspects of cybersecurity.

Public institutions, agencies and initiatives for SMEs are a group of stakeholders who have great capacity to promote, for example through recommendations, the use of tools developed in the GEIGER project, and thus increase the impact of the project. The potential of these target audiences will be mapped and investigated, in collaboration with the consortium partners, on European level, as well as member state and local level, particularly in the pilot use case countries. They could include European institutions, agencies and initiatives for SMEs such as [Executive Agency for Small and Medium-sized Enterprises](#) (EASME), member state government organisations and initiatives for SMEs, and local and regional governments, operators, and policy-makers.

In some countries, there are also, in addition to public bodies and initiatives, semi-public or private entities who are typically offering MSEs and self-employed persons services relating to the administration and day-to-day management of their businesses. For example in Belgium, the "social secretariats", such as [Securex](#), handle a number of administrative tasks for other companies. They are bodies that offer services relating to salary administration, personnel management, and socio-legal assistance, and are also strongly involved when a self-employed person sets up the legal entity to run their business. These bodies offer a potential direct, trusted channel to the key target audience of the GEIGER project, small businesses, and a collaboration with them will thus be investigated further.

A detailed mapping of these stakeholders, and refining the prioritisation of each of them in our planning according to their potential reach towards our primary target audience and their likely motivation to support our actions is critical, to focus our dissemination efforts to those stakeholders that will help us maximise our impact.

2.4.5 Other target audiences

- **CERTs/CSIRTs:** We seek to establish cooperation with national and other computer emergency response teams (CERTs) and computer security incident response teams (CSIRTs) in security information exchange regarding incidents, threat stats, and recommendations. During the project, we will mainly cooperate with consortium partner CERT-RO and third-party CERTs the National Cyber Security Centre (NCSC) in Switzerland and Digital Trust Center in the Netherlands. We strive to involve as many CERTs/CSIRTs as possible in agreeing on the GEIGER Cloud API towards CERTs, i.e. as part of the GEIGER activities contributing to standardisation. We aim at having, at the end of the project (as per KPI I2.1.4.5), CERTs in at least 50% of the EU member states on board and intending to cooperate with GEIGER.
- **Providers of security technology and services:** GEIGER will integrate a number of tools, either protection tools, recommender tools or educational tools, in its toolbox, from both developers within the project consortium and third-party providers. They will be approached to investigate the possibilities and practicalities of the integration.
- **Security experts:** In addition to the expertise possessed within the consortium, we will seek input and feedback from third party security experts throughout the project.
- **Standard setting bodies:** To achieve a functional and usable GEIGER solution, standardisation of both the technical and educational aspects of the project is critical. To this end, we will address standard setting bodies, for people or company labels and certificates (such as [ICT Berufsbildung Schweiz](#) and [ISQI](#)).

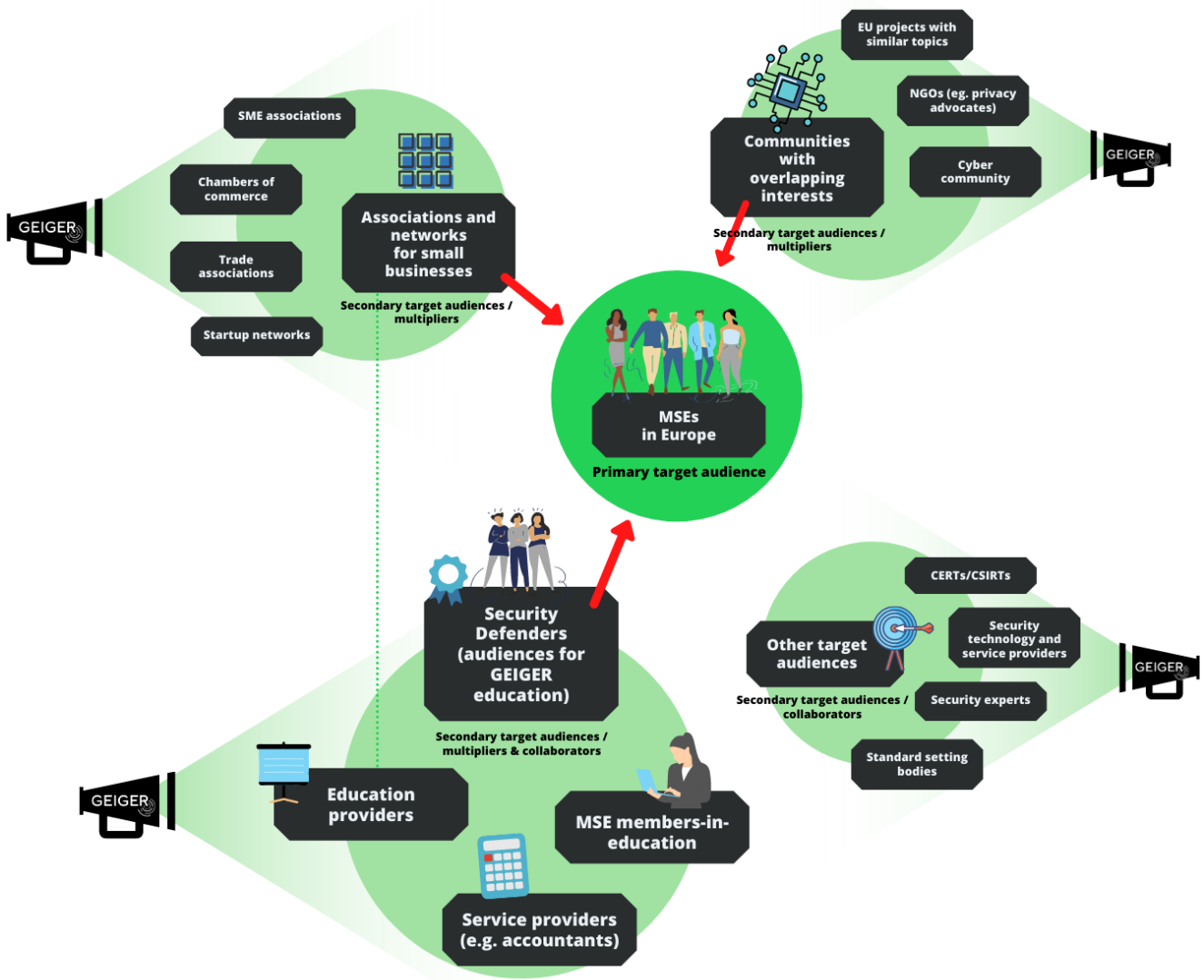


Figure 3: Target audience and multipliers

2.4.6 Priorities for engaging target audiences

To use our limited resources in a way that maximises the impact of the dissemination and communication of the project, building a strategy based on prioritising certain target audiences is necessary. While the end-users of the GEIGER Solution, small businesses, remain the obvious primary target audience, the focus of the communications efforts will shift from one target audience to another as the project progresses.

To clarify the priority target audiences of our communications, and to allow for efficient utilisation of leverage for maximum advantage, we are using the Mendelow's power/interest matrix. It helps mapping the power (the ability to influence whether the project will reach its goals), and interest (the likelihood or motivation to use their power to influence the outcomes of the project and its dissemination) of each stakeholder towards the GEIGER project. In this exercise, we focus on the targeted key multipliers of our dissemination and communications, and based on it, we define four different levels of engagement with these stakeholders, and gain a better understanding of the efforts that should be allocated for communicating with each of them:

- A. **Minimal effort:** These stakeholders are not particularly interested in the project and do not have much power. The chosen approach is to ensure limiting the resources used towards serving these stakeholders, while still being aware of their existence.
- B. **Keep informed:** These stakeholders have a high level of interest in the project, but lower power. The chosen approach is to keep these stakeholders informed of plans and outcomes of the project.
- C. **Keep satisfied:** The stakeholder has a high ability to influence the project, but currently low interest in it - if dissatisfied, their interest level may rise and they will influence in a negative manner to the success of the project. The chosen approach is to keep them satisfied, however without excessive efforts.
- D. **Key players:** These stakeholders have high influence and they are highly motivated to express their own interest. The chosen approach is to involve them and encourage their participation in the project from an early stage, to integrate their goals and ensure their support.

The following figure shows the key stakeholders of the GEIGER project, from the perspective of its dissemination and communications, placed on the Mendelow's matrix:



Figure 4: Level of stakeholder engagement, Mendelow's power/interest matrix

2.5 What: Key messages

The GEIGER vision has been, simultaneously to this Impact Plan, formulated as part of the work in WP1. This overall vision plays a major role in the goals of the dissemination and communications of the project, and consequently in the choices of messaging.

To raise awareness around the project among our target audiences, to engage them and convince them to act, in order to create the desired impact, it is essential to define the framing, the key messages, and the value proposition we wish to communicate. To do that, we need to understand what our target audiences' interests and values linked to GEIGER are, and what the unique benefits of engaging with GEIGER could bring them. It is also crucial to carefully consider what our target audiences need or want from us, instead of focusing on what we want from them. To build a coherent framing and messaging, the overarching message for all our target audiences has to be the same. However, to appeal to our very varying secondary target audiences, and for our communications to result in the desired action, the nuances of the messaging have to correspond to the needs of each target group. The messaging around the project will be customised, while maintaining the red thread of it, for the planned campaigns towards different target audiences, according to the specifics of each of them.

For example, to raise awareness on the project and the GEIGER solution among MSEs, our primary target audience, and to engage them and convince them to act, it is essential to understand what are typically the major obstacles for small businesses to adopt better cybersecurity practices, and what added value adopting the GEIGER toolbox could bring them. Understanding what would persuade them to dedicate their time and efforts to learning about cybersecurity and taking action to improve their practices is critical when formulating the core of our messaging. For our primary target audience, the messages will be developed in particular around barriers and challenges they are facing, and we will bring the topic closer to them by using appealing storytelling and real-life stories (anonymised, whenever needed) about individuals facing similar problems.

GEIGER's core value proposition for small businesses:
An easy and affordable solution for cybersecurity, and support in its use.

We will be working during the coming months on the detailed framing and messaging for each of our target audiences, taking advantage of the deep understanding the consortium members involved in the pilot use cases have acquired on their audiences, and on the particularities of communicating cybersecurity issues to them. To successfully communicate the project, to reach the level of awareness we aim to reach, and to incite the reaction that creates the desired impact, we will also test and adjust, whenever needed, our messaging throughout the duration of the project, in consultation with the relevant stakeholders.

We will also, in collaboration with all consortium members, formulate a "tagline" for GEIGER, to present the core value proposition of the project and the GEIGER toolbox clearly and concisely. The dialogue to define the wording of this tagline has been started in the WP5 working group.

The table below lists some of the key target audiences, their interests and values linked to GEIGER, as well as barriers and challenges to engage with the GEIGER tool or contribute to the promotion of the project. It suggests key messages and style of communications likely to result in the desired action.

Target audience	Interests & values linked to GEIGER	Barriers & challenges to engage	Key messages / style of communications towards this audience
Small businesses	<ul style="list-style-type: none"> • Avoiding financial losses • Continuity of business • Customer confidence and trust 	<ul style="list-style-type: none"> • “Coping problem” - despite the awareness on cyber threats, no concrete tools to address them, and so concerns are ignored • Lack of time • Lack of expertise • Lack of financial resources 	<ul style="list-style-type: none"> • Relatable and emotionally appealing user stories • Focus on challenges, solutions, and benefits • Emphasising the affordability and ease-of-use of GEIGER, and that no previous knowledge of cybersecurity issues is required
SME associations & networks	<ul style="list-style-type: none"> • Offering tools and benefits to their members 	<ul style="list-style-type: none"> • Competing priority topics 	<ul style="list-style-type: none"> • Pointing out GEIGER’s added value to their members/audiences • Offering attractive and ready-to-use materials for them to distribute
Education and training providers (vocational schools, MSE associations, third party providers)	<ul style="list-style-type: none"> • Offering tools and benefits to their students • Adapting their study programmes to be fit for digital age • Offering a Certification on the topic of cybersecurity 	<ul style="list-style-type: none"> • Competing priority topics • Lack of time/resources 	<ul style="list-style-type: none"> • Offering up-to-date and easily adaptable learning materials • Giving an overview on materials and organisation of the GEIGER education • Offering support and exchange (e.g. within the Education Provider Community)
Security Defenders (Low-Level)	<ul style="list-style-type: none"> • Increasing the personal cyber resilience within the MSE and to some extent the general MSE cyber resilience 	<ul style="list-style-type: none"> • Lack of time • Little confidence on the cybersecurity subject • Limited awareness on the subject 	<ul style="list-style-type: none"> • Offering compact and valuable trainings • Highlighting behaviour as important factor for cybersecurity within the training • Target audiences to be differentiated (age, working field etc.), several channels and communication styles to be adapted

Certified Security Defenders (High-Level)	<ul style="list-style-type: none"> Increasing the general cyber resilience and awareness of the own MSE Offering help in cyber resilience to other MSEs 	<ul style="list-style-type: none"> Lack of time Lack of interest (e.g. being already part of other programs or established structures) 	<ul style="list-style-type: none"> Offering compact and valuable trainings Highlighting the Certification
Communities with overlapping interests	<ul style="list-style-type: none"> Similar goals/ideals Economic and social benefits of GEIGER Offering tools and benefits to their audiences 	<ul style="list-style-type: none"> Agenda/views not entirely matching to ours Lack of motivation to promote our contents without direct benefits from it Competing priority topics 	<ul style="list-style-type: none"> Highlighting the common goals and the added value GEIGER could offer for them to reach their goals Using vocabulary and terms matching to their communications in our direct exchanges with them Pointing out GEIGER's added value to their members/audiences Adapting to the formats of communications and producing contents and materials that fits to that
Other audiences: CERTs/CSIRTs, tool developers, service providers, security experts, standard-setting bodies	<ul style="list-style-type: none"> Similar goals Potential benefits of GEIGER Offering tools and benefits to their audiences 	<ul style="list-style-type: none"> Lack of motivation to promote our contents without direct benefits from it Competing priority topics 	<ul style="list-style-type: none"> Target audiences to be differentiated, varying channels and messaging to be adapted

Table 5: Key target audiences, their interests and values, and barriers engage

2.6 How: Tools, channels, activities, materials

To efficiently reach each of our target audiences, and to interact with them in a meaningful way, we will use a mix of various communications channels and tools - digital, print, and face-to-face.

The existing channels, tools and contacts of the consortium partners are the backbone of the GEIGER dissemination and communications. The dissemination lead, Tech.eu, has a reach of approximately 70 000 viewers for its website, 50 000 for social media accounts, and 11 000 for its newsletter, and the readers are mainly from the tech start-up ecosystem, which is an important part of the target audiences of the GEIGER project. These channels will be used to reach the local audiences, in particular in the pilot use case countries. The channels and tools being used vary from one consortium partner to another, and the mapping of the roles, channels, communications resources and expertise of the partners that was conducted as part of kicking off the dissemination of the project (see 'Internal organisation of dissemination and communications work') will facilitate

the efficient use of these channels and tools, and support the creation of materials and the coordination of actions fit for the purpose, to maximise the impact and to guarantee the efficient use of our resources dedicated to the dissemination of the project.

Logo and style guidelines have been created to unify the visual communications and to facilitate building brand recognition for the project and the GEIGER tools.

The channels and tools specifically created for the GEIGER project are the website, newsletter mailing list, and social media channels. As these channels have been built from scratch, to gain the audience and build up their follower-base, collaboration and encouraging active promotion of these channels via the consortium members' existing channels is critical. The contents on these channels will be published mainly in English - mother tongue of only a tiny fraction of our primary audiences - so their reach is limited, and only more targeted and local social media actions by consortium partners will assure the desired reach.

The press and media work of the project relies heavily on the local efforts in the countries where GEIGER consortium members are active. However, in addition to that, the dissemination lead aims at building contacts with and bringing the project to the attention of journalists working for the most relevant European media outlets, to gain visibility in publications and broadcasts targeted to the audiences interested in the EU affairs and European-level decision-making.

Awareness among the target audiences on the GEIGER project and its activities will also be raised during relevant events. This will be done on one hand by the organisation of events as part of the project's core activities, and on the other hand by the participation in external events, and the collaboration with event organisers for example by co-organising panel discussions or workshops within an external event.

2.6.1 Visual style

The visual style of the GEIGER project is an important aspect as it is the first touchpoint with our audiences. A visual style and identity showcase core values, a brand vision and future goals. This creates an impact on onboarding consortium members, new collaborators, and potential end users of the GEIGER toolbox as it promotes a sense of direction.

Core values of GEIGER:

Simple. Clean. Clear. Friendly. Understandable. Reduced. Lightweight. Modern. Innovative. Professional. Trustworthy. Reliable. Transparent. Secure. For Everyone.

The visual style is also a crucial foundation for brand awareness and brand affinity. Brand awareness means that potential partners and end users become familiar with the GEIGER project, its values, its services, and the added value they might offer. The consistency of the visual style also ensures that our project will stand out through repeated recognition. The ability to recall and recognise the GEIGER project because of a cohesive visual style increases the brand affinity. As the trust in the project rises, the visual style helps in acquiring new partners and in establishing collaborations.

2.6.2 Website

The website for the GEIGER project, <https://cyber-geiger.eu/> (or <https://project.cyber-geiger.eu/>) offers a unique focal point for communicating the project to all its stakeholders, and to allow the visitors to find the details of interest and relevance to them.

The website introduces the project and the consortium behind it. It documents the progress of the project, listing the deliverables, publications, press releases, and events - both upcoming and past - and allows the interested audiences to get in contact with the contact points of the project, and to express their interest in receiving news regarding GEIGER.

GEIGER

Home Framework Project News & Events Contact

GEIGER

Solution for small businesses to protect themselves against cyber threats

SMEs and micro-enterprises are increasingly "going digital". This also increases the likelihood of incidents due to negligence or malicious attacks. It's crucial that these small businesses are aware of their risks related to data protection, privacy, and cybersecurity, and get help in reducing them. There are plenty of solutions available, but they don't match the needs of small businesses with no expertise in digital technologies or resources to invest in costly and complicated solutions.

GEIGER, an EU-funded Horizon 2020 innovation project, aims to close this gap. The project will develop a "Geiger counter" for cybersecurity, which dynamically shows the level of current risks for the company, and allows the user to take simple measures to lower the risk exposure significantly. GEIGER also aims at building an ecosystem of competent individuals and organisations that offer help, by collaborating with schools and partners to develop a standardised learning programme, the "Certified Security Defenders".

GEIGER framework

SMEs & MEs in Europe

GEIGER indicator

GEIGER toolbox

SME & ME Associations

Networks of excellence (CERTs/CSIRTs)

GEIGER Cloud

GEIGER education ecosystem

Education provider community

Certified Security Defenders

Educated & Certified Security Defenders Community

LATEST NEWS AND EVENTS

#CybersecMonth: Let's talk about digital security!

October marks Cyber Security Month, and we took this chance to talk about what cyber threats we face every day and how we could avoid them. It might seem that cyber attacks are far away from us or our business and present the greatest danger only for large corporations. Unfortunately, the statistics say otherwise. Almost half of all the threats strike small businesses. The most common attacks among them are web-based and social engineering attacks, as well as phishing. [→ read more](#)

Cluj Innovation Days, GEIGER panel discussion

The GEIGER project was introduced in a Cluj Innovation Days panel discussion "Increasing the digital resilience of small businesses - GEIGER counter for cybersecurity" on 12 October 2020. [→ read more](#)

GEIGER Dutch use case workshop

The Dutch use case workshop Workshop for the GEIGER Horizon 2020 project to discuss the background and opportunities for SMEs and accountants [→ read more](#)

[MORE NEWS](#)

Figure 5: GEIGER project website, frontpage

2.6.3 Social media

Today, in particular considering the recent switch towards digital in most areas of our lives, social media platforms have become an important extension of our "public space". Even though the social media channels are not the focus of the GEIGER communications, and reaching our primary target audiences through these channels is relatively uncertain, the presence of the project on these platforms is necessary. Social media platforms will be used for announcing the news, updates and progress of the project, but also for sharing contents produced by others related to the topic of the project and relevant for our audiences, such as cybersecurity and privacy tips, and for participating in the public debate around these topics.

We also aim to use social media platforms as a channel to connect with our secondary target audiences, such as communities with overlapping interest (see 'Who: Target audiences'), to collaborate in sharing each other's contents, as well as to contribute to relevant campaigns, search for contributions to our communications campaigns and actions, and to participate in public debate on the topic of the project on these platforms.

The GEIGER social media channels ([Twitter](#), [Facebook](#), [LinkedIn](#), [Instagram](#), [YouTube](#)) have been created at the beginning of the project, and building up the follower-base is the first challenge. During the early stages of the project, we will focus on organically growing our social media audiences by encouraging the consortium members to actively promote the project via their respective channels, and to share the posts done through GEIGER channels. We will analyse the results and evaluate the success of this approach and adjust our social media strategy accordingly. In later stages of the project, when action is desired from the target audience and we will aim at extending our reach towards a wider European audience, also paid visibility via social media channels will be considered.

The contents on these social media channels will be published mainly in English. The challenge is that English is the mother tongue of only a small fraction of our audiences. Even if today, it is common for especially younger generations to comfortably communicate in English, our primary target audience includes many who do not understand it, or have a strong preference for their native language, and communications in English will consequently not reach them. To address this challenge, and to assure the desired reach, the dissemination lead will facilitate and support targeted and local social media actions by consortium partners. This will be done for example by preparing easily customisable templates of the campaigns and actions run via GEIGER social media channels, which will allow running the translated and adapted campaigns for local audiences.

2.6.4 Newsletter

The GEIGER newsletter will be an electronic newsletter sent out periodically. The frequency of these mailings is to be defined during the next stages of the planning of communications actions, and will relate to the progress of the project, and the available and relevant contents to communicate. It will include updates on the progress of the project and the development of the GEIGER toolbox, events, latest news from the field, and calls for action. The newsletter will allow us to deepen the connection with the interested parties, educate them on the subjects of the project, and prepare them for the launch of the minimum viable product (MVP) of the GEIGER toolbox, to guarantee the reach of the right audiences when an action is desired.

Subscriptions to the newsletter will be possible through a form on the project website, or through a personal request, for example during a one-to-one meeting with a project partner. We also aim at collecting the contact details of the interested subscribers during events, using a GDPR compatible form.

2.6.5 Events

Awareness among the target audiences on the GEIGER project and its activities will be raised during relevant events. This will be done on one hand by the organisation of events as part of the project's core activities, and on the other hand by the participation in external events, and the collaboration with event organisers for example by co-organising panel discussions or workshops within an external event.

The participation in external events, such as conferences, workshops, and trade events, will be an important opportunity to extend our audiences and bring the project to the attention of stakeholders from outside the established circles of the consortium members. To actively promote GEIGER during the events, consortium partners are encouraged to give presentations, to speak in panel discussions or moderate them, to be present in an expo booth, to distribute information and promotional material on the project, and to have one-to-one meetings with relevant stakeholders. The focus will be the events with a potentially interested large audience, and events specifically targeted to small businesses.

We also plan to organise, in physical or virtual format, focused workshops to discuss the topics around the project with the European and international communities, as well as training sessions

targeted to MSEs. These events contribute towards the Impact KPI I2.1.1.10, "GEIGER capacity-building refined in >10 events targeting SMEs&MEs", and seek to involve third parties from outside the project consortium, to utilise their views and contributions to steer the project results towards a genuinely usable and useful solution for its potential users and collaborators, and to guarantee the positive long-term impact. At the end of the project, the final workshop to gather all the stakeholders and to promote and collect feedback regarding the launch of the GEIGER organisation will be organised.

Events constitute also a natural opportunity for being active on social media, to reach audiences of those events by the use of connected hashtags, and making the participants and organisers of the event aware of the GEIGER project by tagging them to our social media posts. The major events might also offer opportunities for media visibility, and chances to connect with media that have an interest in the topic of the event.

To map the relevant upcoming events, a spreadsheet to collaborate among the consortium partners has been established to NextCloud, the file sharing platform of the project (see 'Internal organisation of dissemination and communications work'). This spreadsheet will be used to evaluate the best opportunities to promote the project, and to spot where support for consortium members, for example in terms of the production of promotional materials or speaker preparations, is needed.

The table below lists some examples of the international key events that will offer a potential opportunity to promote the GEIGER project, particularly in the cybersecurity, data protection and privacy communities, through participation and one-to-one meetings, networking, and presenting the GEIGER project in panel discussions, roundtables, lightning talks, workshops, expo booths etc. The initial mapping on the most relevant upcoming events and their prioritisation is ongoing and will be included in the planning once finalised. In addition to the events with the focus on digital security, our target will be on the events that will allow us to reach small business owners and employees first in the pilot use case countries, especially through the cooperation with our identified multipliers, and in the later stages of the project beyond the pilot countries.

Event	Date(s)	Location	Type of event	Target audience
CDPD Computers, Privacy and Data Protection	27-29/01/2021	Brussels, Belgium / online	Conference	Academics, lawyers, practitioners, policy makers, industry and civil society
The Trinational Cybersecurity Days	18-20/02/2021	Basel, Switzerland / online	Conference	SMEs
CSIT 2021 - 8th International Conference on Computer Science and Information Technology	24-25/04/2021	Copenhagen, Denmark	Conference	Academia, industry

Network and Information Security (NIS 2021) Summer School	04-28/05/2021	Crete, Greece	Summer school	Policy makers, decision makers, academia
Cybertech Europe 2021	28-29/09/2021	Rome, Italy	Conference	Industry
Cluj Innovation Days 2021	tbc	Cluj-Napoca, Romania	Conference	SMEs, start-ups, academia, industry
Cyber Security & Cloud Expo Europe Virtual 2021	21-24/11/2021	Amsterdam, Netherlands	Conference	SMEs, start-ups, marketing specialists
FIC International Cybersecurity Forum	04/2022	Lille, France	Conference	Policy makers, industry, academia
Network and Information Security (NIS 2022) Summer School	tbc	Crete, Greece	Summer school	Policy makers, decision makers, academia
Cluj Innovation Days 2022	tbc	Cluj-Napoca, Romania	Conference	SMEs, start-ups, industry

Table 6: Potential international events to promote the GEIGER project

Due to the current COVID-19 crisis, the majority of the physical events have been cancelled, postponed, or converted into online or hybrid events, which constitutes a major challenge for awareness-raising on the project and networking to build relevant contacts and alliances through event participation. Additionally, to set up the internal collaboration within the project consortium, we were forced to shift almost entirely to the virtual environment, and to rely on remote connections. In the absence of face-to-face meetings, special efforts were required to successfully run the kick-off meeting of the project, as well as the first round of use case workshops for the pilots in Switzerland, Romania and the Netherlands, and to set up the framework for the internal communications and coordination of work, and to define the best tools and practices.

The continuing limitations to physical events and meetings pose a risk to the efficiency of raising awareness of the project via this channel. To mitigate the risk, we will 1) carefully investigate the best practices for replacing some of the planned actions in physical events with online and virtual activities, and 2) dedicate more efforts than initially planned to other areas of communications, such as connecting with our audiences through targeted and mass media.

2.6.6 Mass media

Mass media has a major role in the communications strategy of the GEIGER project. A significant percentage of the population is typically employed by small businesses, and consequently, mass media offers a great potential to reach the part of our primary target audience, small business owners and staff, who are difficult to reach through the commonly used digital channels such as social media.

GEIGER will pursue a mass media-oriented communication strategy previously proven efficient in reaching small businesses (as a significant percentage of the population is typically employed by SMEs&MEs), by targeting national and local television, radio and newspapers, as well as targeted publications such as trade magazines relevant for small businesses in the countries in which the GEIGER project is active. A particular focus will be the collaboration with media in the three pilot countries the Netherlands, Switzerland, and Romania.

We aim at reaching our primary target audience through mass media such as national and local television, radio and newspapers, but also targeted publications such as trade magazines relevant for small businesses in the countries in which the GEIGER project is active. In the early stages of the project, the focus will be the collaboration with media in the three pilot countries the Netherlands, Switzerland, and Romania, and later in the project extended to other European countries.

The following table shows some of the key media outlets we intend to target, to reach our goals related to mass media visibility. The list will be extended when the mapping in cooperation with the pilot use case leads and other consortium partners advance:

Media outlet	Geographical focus	Media format
Deutschlandfunk	Germany/Switzerland	Radio / online news
Heise	Germany/Switzerland	Press / online news
SRF	Switzerland	TV
Het Financieele Dagblad	The Netherlands	Press / online news
Stirile Transilvaniei	Romania	Online TV
TVR Cluj	Romania	Regional TV
Euronews	Europe	Online news, TV
Europe by Satellite (EbS)	Europe	TV
Politico Europe	Europe	Online news
Euobserver	Europe	Online news
EurActive	Europe	Online news

Tech.eu will coordinate and facilitate the production of short videos, press reports, editorial and opinion pieces, in cooperation with the local networks in the countries of the consortium partners. Also, other media formats will be investigated and considered.

Taking into account the diverse languages, cultures, varying media landscapes, and other particularities of each country, the close cooperation with the pilot use case leads and other consortium members actively involved in the dissemination efforts of the project, as well as the exploitation of their understanding of the local environments and existing media connections is critical for guaranteeing the success of this approach.

Tech.eu will coordinate the drafting of traditional actions to reach out to the media outlets, such as joint press releases. Tech.eu will collaborate with the consortium members actively involved in the dissemination and communications work of the project to define the most appropriate and efficient formats for approaching media in their local environment as well as the framing and messaging appealing to them, and based on this, produce templates for the use of the consortium members, and offer support in customising their communications towards media. These templates could include pre-written op-eds or opinion pieces to be published in the collaborating publication or briefings to provide the media with background information both on the GEIGER project and the connected issues in general, among other formats. The support could include for example help in their preparations for media appearances or interviews.

To offer an easy starting point for the journalists, the [Media Kit](#) on the GEIGER website includes a summary of the project, relevant contacts for further information and links to GEIGER social media

accounts, as well as the basic visuals to support their reporting on it. It also lists all the press releases that have been and will be published in the context of the project.

2.6.7 Academic publications and channels

The results of the GEIGER project will be presented and disseminated through publications in scientific journals and conferences and workshops. These publications aim at collecting expert feedback about the quality and soundness of the work being done within the framework of the project, gaining visibility for the GEIGER project among researcher communities and identifying further partnerships, as well as building the reputation of the project and its academic consortium members.

The GEIGER project aims at developing a dynamic and reliable GEIGER Indicator which can be deployed and validated in daily practices of MSEs. This is a highly relevant topic, as security metrics research is more timely than ever, with both the EU – through ‘The EU Cybersecurity Act’ – and the US – through the ‘NIST Small Business Cybersecurity Act’ – stressing the importance of being able to measure the (relative) level of security of cyber-systems, specifically that of SMEs. Nevertheless, a large gap exists between security metric solutions in research, and those put into practice.

GEIGER consortium member UU leads to bridge this gap in the project, and aims to publish peer reviewed conference and journal papers to further the scientific body of knowledge, including those in the following tentative list of research publication topics:

1. Reviewing the cyber-systems metric landscape. Which metrics exist, but also on how universally they can be applied and whether they have been used in practice. This will allow us to answer an important question in our research: ‘Can one assess the security risk faced by any enterprise cyber-system, using a universal set of practicable metrics?’
2. Evaluating cybersecurity risk assessment solutions. An inherently problematic task as participating SMEs will most likely suffer from the observer effect. Additionally, the lack of materialising cybersecurity threats puts us in the challenging setting of rare event modelling. We therefore will report on a novel evaluation strategy for our situation.
3. Enriching and augmenting cybersecurity knowledge using Knowledge Graph modelling; for both the Indicator and the Education ecosystem. We hypothesise that a Knowledge Graph of the cybersecurity for SMEs domain will be able to enrich the GEIGER Indicator metrics as well as better inform the Education ecosystem by providing relevant contexts for cybersecurity entities.
4. Modelling evolving organisational cybersecurity risk. The dynamic setting of cybersecurity leads to a manifestation of concept drift, which the Indicator model should be able to accommodate. Additionally, it should allow for the aggregation of data from a device level to an enterprise level, meaning we will encounter the well-known aggregation problem.
5. Deploying and validating the GEIGER solution in daily practices. We will apply the evaluation strategy for the developed software solution and test it in various SMEs in diverse sectors over multiple countries.

Academic impact of this research includes providing a holistic overview of cybersecurity metrics, developing a novel metric that builds on peer-reviewed elements where possible, while adding several novel components such as an integrated knowledge graph module, and including a scientifically sound empirical validation in SMEs throughout various sectors in Europe. This significant academic impact will provide a Foundation of Trust in the GEIGER solution as a key societal impact.

In its research linked to the GEIGER project, the consortium lead FHNW (Brugg/Windisch) will focus on the problem of the resistance to the adoption of cybersecurity tools and the lack of

compliance with security advice. To make the information security measures more effective and support adherence to cybersecurity practices, bridging the communication gap between security experts and non-experts is recommended. FHNW intends to improve cybersecurity communication, inform employees in SMEs, and encourage small businesses' adoption of good practices:

1. Systematic review. To solve the problem and impact upon cybersecurity adoption, we need to find out the current state of the studied and validated behavioural theories in the context of micro, small, and medium-sized enterprises. Since this knowledge is not readily available, we are researching and reviewing the relevant papers to make novel theoretical and practical insights for the Geiger project.
2. Solution evaluation. To get a more nuanced understanding of cybersecurity meta-requirements for awareness-raising in SMEs and better approaching cybersecurity competence, we are doing inductive theorising through qualitative interviews. The study has a significant addition to our knowledge and has an impact on the Geiger project about approaching cybersecurity in various types of SMEs.
3. Interface validation. To validate the designed interface between MSE and Geiger cloud, we want to know if the prototype supports better user interaction, security management, least resistance for adoption, and influence MSEs' users to have desired cybersecurity behaviour.

In its planned research related to the GEIGER project, FHNW/HSW (FHNW School of Business, Basel) will focus on data privacy and risk awareness for small businesses. Their research will address the issue of the collection and use of often sensitive personal data in today's highly connected world, and the lack of awareness and understanding of risks related to the integrity, confidentiality and availability of this data, especially among small, micro enterprises and private users.

In context of the GEIGER project, they aim to publish peer reviewed conference and journal papers to contribute to the scientific body of knowledge with the following tentative list of contributions:

1. CySecEscape 2.0 - A Virtual Escape Room To Raise Cybersecurity Awareness. 2020. www.mdpi.com/journal/information. Accepted
2. (Virtual) learning games to raise awareness for example about knowledge of current threat situations, impact of social engineering, phishing, secure passwords, etc.
3. Measures and tools to enhance data privacy in small businesses
4. Learning scenarios for different groups, in different contexts
5. Community building theories, frameworks, and its adaption to the GEIGER, MSE context
6. Meta level: Project management in an international consortium under unpredictable COVID-19 situation/restrictions and use of digital, virtual meeting platforms
7. To be elaborated: submit a policy recommendation

Publishing will potentially take place in collaboration with PHF for selected topics.

The topics listed above serve as examples of the scope intended to be covered within the context of the project, and details of the potential publications and dissemination actions supporting them will be further discussed between the academic project partners and the WP5 lead. Ideally, collaboration between the academic project partners will result in collaboration leading into joint research and publications.

2.6.8 Promotional and information material

The purpose of the print materials is to support the introduction of the GEIGER project in the physical events and meetings, and to allow presenting the project in a consistent and unified manner, both in terms of visual style and contents, and to contribute to the image of a reliable and state-of-the-art but simultaneously easy-to-approach tool for cybersecurity, to successfully build trust on the GEIGER project and tools.

Tech.eu coordinates the drafting and production of the print materials, collaborating with the consortium partners. Most of the print materials will be printed locally by the consortium members, to allow them to be customised for the intended use and to match with the needs of each partner.

Some of the planned print materials are a flyer or a factsheet to introduce GEIGER in a concise manner, detailed brochures, roll-ups to be used in physical events as well as on the background of any virtual event or meeting to increase our brand recognition, and branded promotional giveaways. We also aim at publishing a whitepaper for tool developers to introduce the benefits of the collaboration with the GEIGER solution and explain the integration with it, and another whitepaper targeting the SME and professional associations.

2.6.9 Overview of tools, channels, activities, and materials per target audience

The table below shows the key channels, tools, and activities, as well as the type of contents and materials we will aim at producing for each target audience, to support the communications activities towards them.

Target audience	Key channels, tools, activities to reach this target audience	Type of contents and materials to produce
Small businesses	Mass media	High impact stories, press articles, op-eds/opinion pieces, videos, background briefings
	Social media	Social media campaigns and actions
SME associations & networks	Events	Print and digital materials to introduce GEIGER and to support building brand recognition, panel discussions, keynote speeches, training/educational materials
	Collaboration for publications	High impact stories, press articles / blogs, videos, social media campaigns
	Direct contacts	Print and digital materials to introduce GEIGER
Security Defenders / audiences for GEIGER education	SME associations & other networks (see above)	Print and digital materials to introduce the GEIGER education, possibly a mock-up of game or similar
	Events	Print and digital materials to introduce the GEIGER education, possibly a mock-up of game or similar, keynote speeches, panel discussions
	Social media	Social media campaigns
	Relevant communities (online)	Print and digital materials to introduce the GEIGER education, maybe mock-up of game or similar

Communities with overlapping interests	Social media	Social media campaigns and actions, direct messages to introduce GEIGER
	Events	Print and digital materials to introduce GEIGER and to support building brand recognition, panel discussions, keynote speeches
	Direct contacts	Print and digital materials to introduce GEIGER
Other audiences (CERTs/CSIRTs, tool developers, service providers, security experts, standard-setting bodies)	Events	Print and digital materials to introduce GEIGER and to support building brand recognition, panel discussions, keynote speeches
	Direct contacts	Print and digital materials to introduce GEIGER
	Relevant communities	Print and digital materials to introduce the specific aspect of GEIGER

Table 7: Overview of tools, channels, activities and materials per target audience

2.6.10 Partners' roles

The organisations involved in the GEIGER project, extremely varying in their size and field of activity, offer us an outstanding range of possible contributions to the dissemination and communication of the project.

Associations and clusters of small businesses (such as SKV, SRA and ClujIT) will use their established publications to reach our primary target audience and contribute to building of the framing and messaging that appeals to their respective audiences. They will be also offered a great opportunity to test and adjust the best ways to reach our primary target audience and provide us with feedback regarding the success of our communication actions among their audiences.

MSEs involved in the project (such as e-abo, Coiffure Loredana, Public Tender, and Braintronix) will provide us with their experiences around cybersecurity, privacy and data protection, and offer us an insight of the challenges they have faced, and the solutions GEIGER could bring to these challenges. These can be used as elements of storytelling in our communications. The MSEs will also provide feedback regarding the suitability of the messaging towards them and their peers, helping us to communicate in a way that addresses the needs of this audience.

Academic partners of the project (such as UU and FHNW) will contribute to the awareness-raising within the scientific community through their own and potentially joint publications, as well as participation in events.

Education and training providers (such as BBB, PHF, ClujIT and SRA) will collaborate with the dissemination lead in building an approach for communicating the GEIGER Education, to reach out to the potential "Security Defenders", through education providers and directly. Different types of education programmes, from vocational schools to adult education, will be considered in this approach.

Large providers of cybersecurity tools and expertise (such as KSP, ATOS and KPMG) will contribute to the dissemination and communication plan with their specific expertise in communicating around the topics of the project, and with their suggestions for the most efficient tools and channels. They

will also use their established contacts to media and other relevant multipliers to enhance the media visibility of the project and represent the GEIGER project and share their expertise and views as speakers in events.

Tech.eu, as the GEIGER project dissemination lead, handles the coordination of the dissemination and communications actions, creation of the proposed contents and templates that can be customised for different occasions by the consortium members, and tracking, evaluation, adjusting and reporting of the impact of the dissemination and communications actions. Tech.eu handles the day-to-day updates and monitoring through the digital GEIGER channels - social media and website, and is also responsible for the communications towards and building relations with the stakeholders at the EU level such as “EU bubble” media, European associations and networks, and EU's public institutions and initiatives for SMEs.

At the national level the focus is particularly at the early stages of the project on the pilot countries, Romania, Switzerland and the Netherlands. The consortium members involved in the pilot use cases will use their established communications channels and build new relations to relevant stakeholders and media outlets in their countries, to allow raising awareness on the project. The dissemination lead cooperates with them to assure the consistency of the communications, and to provide them with the necessary support to maximise the impact of their communications efforts.

2.6.11 Internal organisation of dissemination and communications work

The project kicked off in the middle of the COVID-19 lockdowns, entirely online. In the absence of the chance of getting to know each other face-to-face, special efforts were required to successfully set up the framework for the internal communications and coordination of work, and to define the best tools and practices.

To kick-start the dissemination collaboration within the consortium, we prepared a [questionnaire](#), using the privacy-friendly Framafoms platform, for each partner to fill in. The goal of the questionnaire was to map the roles and contact details of each person involved in the dissemination and communications aspect of the project, the social media accounts and other channels each organisation could use to promote the project, the relevant resources and expertise they possess to contribute and the role they see themselves playing in the GEIGER dissemination and communications. The responses allowed us to better understand the dynamics of the consortium for the purpose of efficiently coordinating the upcoming dissemination work, and to create the list of contact points in each partner organisation. The mapping of the social media accounts facilitated the connecting of the newly created GEIGER accounts to all consortium partners and the individuals involved on each platform.

As the most important practical tool for cooperation in the early stages of the project, WP5 established two regular meetings (conference calls):

1. Bi-weekly work package task leader meeting to coordinate the work within WP5
2. Monthly meeting for all consortium members involved in the dissemination work to allow everyone to stay updated on the past and planned communications activities, and to collect ideas and contributions.

In addition to these two recurrent meetings, separate meetings are organised to discuss specific actions and activities.

The main communications channel between the consortium members involved in the dissemination and communications work is the dedicated WP5 mailing list, through which any member of the mailing list can raise questions, inform others on their upcoming actions, and comment on the ongoing discussions.

The tool used in the project for file sharing and repository is NextCloud, an on-premises content collaboration platform hosted by FHNW. It can be accessed either via a web browser or can be synchronised with the file explorer. The files related to the dissemination work of the project, such as minutes of meetings, collaborative dissemination tracking spreadsheets, and templates for documents, presentations, and visual materials are shared through NextCloud. On NextCloud there is also a spreadsheet to list white, red, and black lists, to clarify which documents are public (white), confidential (black), and require discussion within the project consortium before their possible publication (red).

To maintain a unified visual style in all communications related to the project, and to make it easy to create customised and attractive visual materials without the expertise of a graphic designer, we also created a shared [Canva](#) folder. Canva is an easy-to-use online tool for design, offering a wide selection of features for creating attractive visuals, in particular for digital use, like social media images and videos and web banners, but also allowing the design of simple print materials. The folder is accessible to all consortium members, and the templates saved in it are accessible to anyone in the "GEIGER team" and can be freely modified for varying purposes. The shared folder is ideal for the visuals that are to be used in "fast" digital publications such as social media posts and online or email banners, but the tool is also convenient for sharing templates for print materials that require modifying in terms of language, logos included, or other details.

To guarantee the efficient use of the communications tools put in place during the first six months of the project, to complement the existing style guidelines and templates, we will establish an "image bank", chosen photos and visuals for the use of the consortium members in the context of the project, and start the production of relevant web banners, video intros, and other visual and audio-visual supports for the project. A brief guide for use of these materials, or a "communications handbook" will also be developed.

2.7 When: Timeline

The planning of the timeline of the dissemination and communications of the project will be affected by the internal developments within the project, external developments, and the resources available.

The internal developments include the milestones of the project such as launches, publications, and deliverables. The external developments include any events that may have an impact on the project or offer an opportunity to reach out to our target audiences, such as industry events, campaigns, or expected publications or launches of reports, initiatives, or consultations relevant to the topics of the project. These internal and external developments will be reflected against the resources available for implementing the communications actions, in any particular point of time and geographical location, if applicable, and based on that, the decision regarding the detailed timeline of the best combination of activities to reach the maximum impact is taken.

The publication of scientific papers and articles linked to the project will be led by the academic consortium partners and supported by the dissemination lead through their promotion via GEIGER channels. FHNW, responsible for the T5.2 Standardisation, will lead the communications related to standardisation and policy activities of the project, and the consortium partners involved in the technical development of the GEIGER toolbox will liaise with the tool providers and security experts for their involvement and engagement. The partners responsible for these areas will define the timeline of their respective communications efforts, and the dissemination lead will support them when necessary.

2.7.1 Project launch & preparation phase (M1-M6)

During the first six months of the project, the dissemination and communications work focused on the internal alignment within the consortium, setting up the tools and practices for efficient collaboration, as well as the branding of the project, identification of target audiences, and starting to initiate relevant contacts and to raise awareness on the project externally. The tools and channels for external communications (website, newsletter mailings list, social media accounts etc.) are gradually set up and start to be served.

The key contents of the communications revolved around the cybersecurity challenges that MSEs are facing, and GEIGER's role in overcoming them. The communications have been targeted, in addition to the internal stakeholders in the project, to their existing contacts and organisations and networks that could be seen as potential multipliers for our dissemination efforts.

2.7.2 GEIGER development and building education provider community (M7-M18)

The M7-M18 of the project marks the development of the minimum viable product (MVP) for the GEIGER toolbox. The principal dissemination objective of the second stage of the project is to generate interest among the communities that will be able to positively impact the success of the project and its dissemination. This stage aims at building the communities of associations and networks that connect small businesses, as well as education providers that will potentially add GEIGER Security Defender education to their study programmes or training offerings. The dissemination kit for the use of the consortium partners, including videos, flyers, poster, brochures, factsheets, market-specific material, and press releases and briefings will be built to facilitate the unified and coherent communications around the project.

The focus of the messaging will be on the potential benefits of the collaboration and adopting of GEIGER to the above-mentioned communities. The most used channels for contributing to building these communities will be the participation in events and collaboration in organising them, encouraging the subscriptions to the newsletter, direct contacts and networking, and to a limited extent targeted publications and mass media.

2.7.3 GEIGER refinement (M19 - M24)

During this stage of the project, the GEIGER MVP will be refined. The dissemination and communications efforts aim at activating the stakeholders to register their interest in GEIGER, by for example subscribing to the newsletter mailing list, signing up for a webinar, or ordering/uploading a resources pack through GEIGER website. As the GEIGER education programme will now be fully developed, this stage also aims at initiating the building of the Security Defenders community.

The communications efforts will relate to the coordination of actions with established multipliers to reach and activate our primary audience, MSEs, and to continuing to build new alliances with potential multipliers. The focus of the messaging will shift from the cyber security challenges for MSEs and benefits of GEIGER to them towards a more pragmatic perspective and a direct call-for-action; encouraging the MSEs to test their cybersecurity practices and to evaluate level of risks, and to sign up for testing GEIGER once the MVP will be rolled out. This will be done using the elements of the GEIGER toolbox already defined, even if not yet launched, and for example mapping the cybersecurity risks of an MSE by asking simple key questions around their cybersecurity practices.

In this stage, we will heavily rely on the targeted publications of our multipliers, and mass media visibility achieved in collaboration with them. Event participation newsletter mailings, website and social media contents, and the production of audio-visual material will keep supporting the efforts of raising awareness around the project. Project outcomes to date will be tested based on liaison with professional and SME associations during workshops.

2.7.4 GEIGER rollout & release (M25-M30)

The last stage of the project will include the release of the GEIGER MVP. This stage allows us to finally communicate the functionalities of GEIGER toolbox and to present the user interface, and the MSEs will be able to test the tools in practice. The GEIGER toolbox (beta version) will be introduced to the end-users, and they will be activated to install and test it, and encouraged to provide us with their feedback. This stage is critical for the project's communications and dissemination, and it will play a determining role in the success of creating the desired impact.

The focus of the messaging will be the functionalities and the interface of the toolbox, as well as the benefits that adopting it offers. This stage targets wide mass media visibility, as well as extended coverage in relevant targeted publications such as trade magazines and SME association newsletters, and the media visibility will be expanded beyond the pilot use case countries. The final workshop of the project to gather together all the stakeholders will be organised, as well as targeted practical workshops, particularly in the context of the pilot use cases, and we will facilitate event participation and collaboration with existing events to present GEIGER. Newsletter and social media actions will support these intensified efforts for visibility.

2.7.5 Post-project

The objective of the project is to prepare the jointly developed GEIGER solution for sustainable rollout, and to guarantee the continuation of the tools and the ecosystem built during the project. The communications efforts of this post-project stage will be to facilitate a successful roll-out of the GEIGER spin-off, and to bring a finalised solution to the attention of MSEs across Europe. The communications plan for this stage will be developed during the project.

2.8 Criteria for measuring success

The criteria of measuring the success of the dissemination and communications efforts of the project will be reaching the listed KPIs. The qualitative feedback collected from stakeholders will also play a role in it.

More detailed objectives for the number of publications and actions will be developed during the next stages of the project. However, these numbers remain indicative and do not constitute an official criterion for measuring the success of the project, as the quality of a publication and a correctly chosen channel defines the actual reach of the publication among the primary target audience and thus its impact more reliably than the sheer number of publications.

2.9 Achievements to date

This chapter describes the progress that has been done until the end of M6 of the project under T5.1. It lists the channels, practises, relations, materials, and infrastructures put in place during M1-M6, and the processes behind them.

2.9.1 Logo and visual style

A logo is typically composed of an iconography or a visual element, a font and a colour. It is a design used to aid and promote public identification and recognition, and it communicates the core concept and values of a brand or in this case, a project. Out of the core values of the GEIGER project we have picked the following five that are important for the logo: simple, friendly, reduced, modern and innovative.

The logo was designed by FHNW, in cooperation with Tech.eu, and consulting the consortium members during the design process and for the final choice of the logo. During the process, several initial ideas were drafted, and two of them were chosen to be elaborated and presented to the

consortium members. One of the logo options was further elaborated into the final logo of the GEIGER project, following the ideas that came up in the internal discussions and comments.



Figure 6: Some of the GEIGER logo options presented during the design process

The GEIGER logo encompasses the whole project. As in the future, the project will expand and have several sub-projects or products, the goal was to develop a visual identity that can accommodate the potential future products.

The iconography of the GEIGER logo is inspired by the element from which the project draws its name, the Geiger counter, a detector that you can point towards an area and check for surface contamination. The Geiger counter is made up of three main elements: a scale, a counter, and audio, all of which give feedback on how many particles there are on the surface area. The element chosen for the GEIGER logo iconography is a round dot, symbolising the specific area that the counter probes.

The logo of the font, TT Norms, is geometric, has a wide implementation range, and is very readable, and thus corresponds to the core values listed above. It is a universal font that fits together with nearly all other fonts. The font has been combined with one visual element, the counter needle, that symbolises the simplicity of which small businesses can see how threatened they are against cyber attacks.



Figure 7: GEIGER logo

The colours of the logo are black (font) and two shades of green (dot). The secondary colours, to be used in documents, presentations and other materials, mainly on the background for gradients, are red and yellow, also in two shades. These three colours are the standard colours for risk communication in Europe: red - very high-risk, yellow - high to medium risk, and green - low risk. As one of the goals of GEIGER is to communicate risk, these three colours are a logical choice. The shades of green were chosen as the principal colour of the logo to communicate the risk in a positive manner.

For the logo applications, it is very important that the logo is applicable, readable, clear, and suitable for both digital solutions and printed media. For the use in digital channels, the logo can be static, animated, or with sound. In print media, the logo is static. There are three colour variations of the logo. The choice of the GEIGER logo depends on the background and production method. For

white backgrounds, the full colour version or the black and white logo can be used. When using the logo on a coloured background, it is possible to choose either the black and white logo with black text or white text.

The [style guidelines](#) were created to demonstrate the correct use of the logo and the other elements of the visual style of the GEIGER project. This ensures a consistent communication for the GEIGER project for strengthening our visual brand, as well as being able to quickly onboard new partners. The guidelines are for both internal use of the project consortium, and for journalists and collaborating partners, and they can be found in the [Media Kit page](#) of the website, as well as in the file sharing platform of the project, NextCloud.

To ensure a consistent and uniform visual style, a set of templates was created for reporting or other formal documents, minutes of meetings, and presentations. These templates provide a predetermined layout and structure which the project consortium can use for their documents and presentations related to the GEIGER project. As well as solidifying brand awareness, templates ensure that project members can focus on making and filling content instead of formatting documents. The templates were designed to be usable for multiple operating systems, as well as being legible on screen as well as in colour or black and white print.

To develop the templates, we first evaluated which documents would be most used. Then the GEIGER visual style was applied to those documents. During the process, there was one iteration in which legibility and the specific colour palette (red, yellow, green) were refined particularly for printing.

All dissemination and communications materials, print and digital, within the project must include the following funding acknowledgment:



This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 883588 (GEIGER). The opinions expressed and arguments employed herein do not necessarily reflect the official views of the funding body.

2.9.2 Website

The GEIGER project website, <https://cyber-geiger.eu> (or <https://project.cyber-geiger.eu>), aligns the same core values as the GEIGER logo: simple, modern, transparent. It is lightweight and can be viewed on different viewports (mobile, tablet, and computer). The website offers an easily approachable overview of the GEIGER solution, the project, the consortium behind it, and its deliverables and publications. It also allows interested stakeholders to easily initiate an exchange with the contact points of the project through the contact form and the listed social media links, emails and phone numbers, and offers media a brief introduction of the project and access to supporting visual materials. The “News & Events” tab allows the visitor to find out about the latest developments and highlights of the project and view the list of the upcoming events in which the GEIGER project will be present. As soon as the newsletter mailing list will be set up, there will also be a form added to the website, through which visitors can subscribe to the newsletter.

The website is built with JBake, a static site/blog generator. JBake is not a content management system (CMS), which means that to create contents and to add them to the website, a certain level of technical knowledge is required. Despite this being an inconvenience for the daily management of the site, with JBake we avoid the serious disadvantages of the CMS solutions. CMS solutions such as WordPress, can result in various security issues, through the use of plugins or badly programmed themes. Using JBake, we have complete control over code, content, and design of the website, which is a choice that is a fit for a cybersecurity project like GEIGER.

However, the effort to manage the website, including the publication of content, implementation of functionality (for example for forms), is increased. Those managing the website and publishing content must be familiar with HTML, CSS, programming, and version control tools.

The core of JBake are markdowns that are mapped to groovy templates. Markdowns contain attributes such as "Header", and "Description". These are mapped to the counterparts in the templates during the "baking" process. Baking is the process of mapping Markdowns to templates and building up all resources for the website.

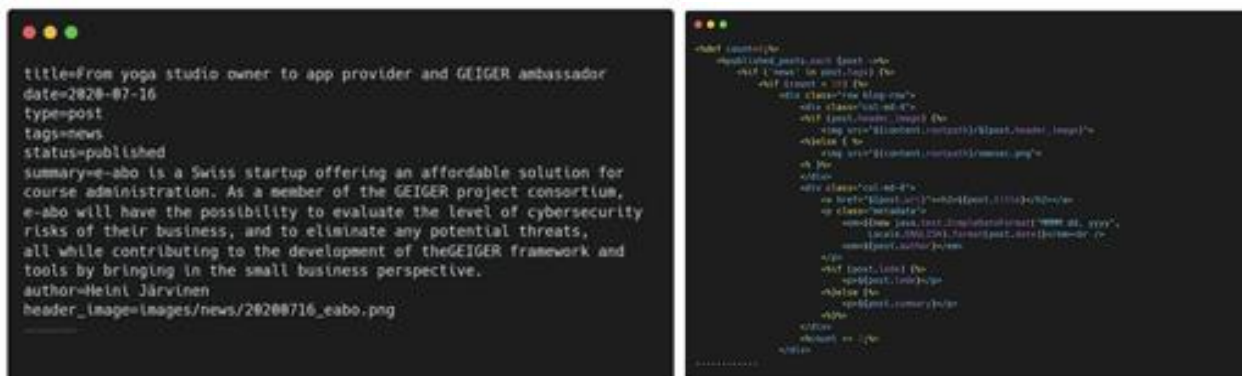


Figure 8: Example of a news markdown header and the corresponding groovy template

The first short article to introduce the actors involved in the pilot use cases of the project, '[From yoga studio owner to app provider and GEIGER ambassador](#)', was published on the GEIGER website on 16 July 2020. As we advance in the collection of contents to communicate the pilot use cases, the next step will be to develop an additional page under the "Project" menu for showcasing the stories of the consortium members and partners involved in the pilot use cases, and highlighting real-life experiences that are relatable for our target audiences.

2.9.3 Social media

The social media accounts for the GEIGER project - [Twitter](#), [Facebook](#), [LinkedIn](#), [Instagram](#), [YouTube](#) - were set up during M1, and communications through them started immediately. As soon as the visual style guidelines for the project communications were consolidated (M4), the social media channels were updated to reflect them.

The kick-off meeting of the project, the presentation of the first scientific paper related to the project, and the use case workshops in the pilot countries were reported and documented in real time through Twitter, Facebook and LinkedIn posts. The travel restrictions due to COVID-19, which resulted in these events being organised mainly online, also complicated the practical implementation of the social media posts around the events, in particular regarding the gathering of visual and audio-visual materials, but this was mitigated by efficient coordination between the consortium partners involved in the organisation of the events.

During M6, we ran a social media campaign, on the occasion of the European Cyber Security Month, to promote awareness on cybersecurity risks among small business owners, and to introduce some of the key concepts and skills to acquire in order to lower the risks. The campaign was published on the social media channels of the project, under the GEIGER branding, actively shared by the project consortium, and raised interest around the topic of cybersecurity and the GEIGER project. It was also a useful first experience in collaboration for such campaign, and the lessons learnt in the process will be used to streamline the planning of the future actions.

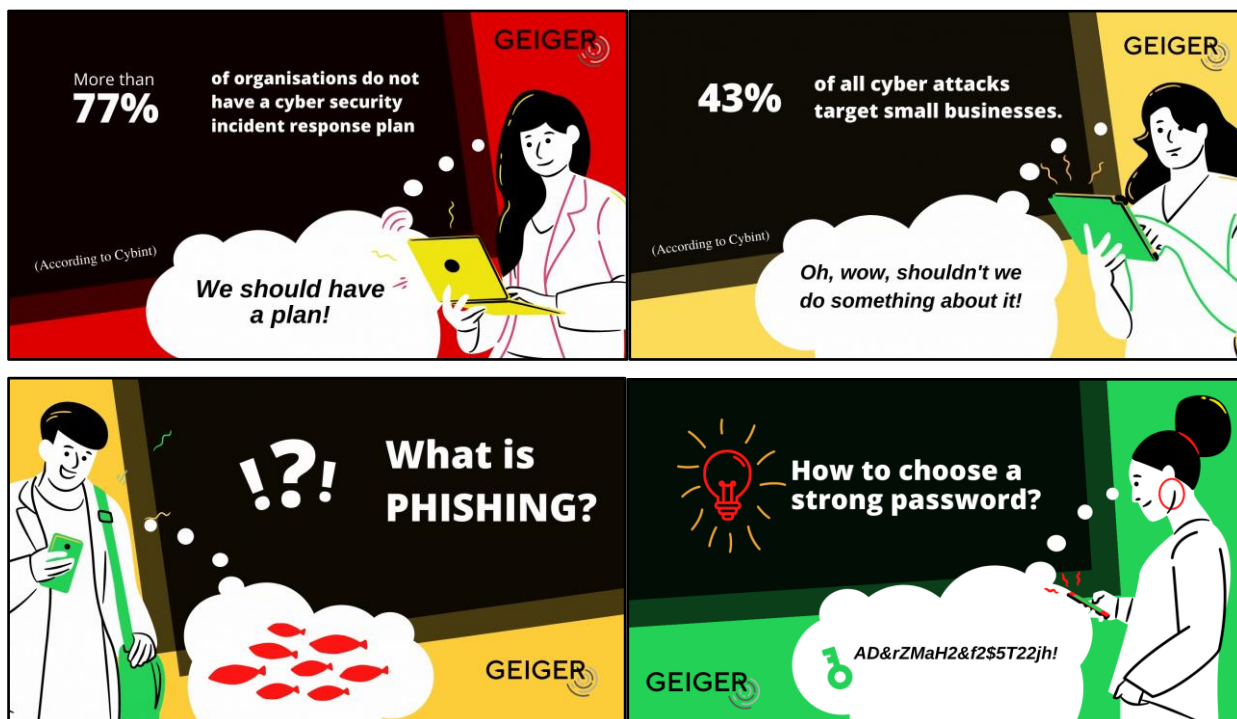


Figure 9: GEIGER social media campaign on the occasion of the European Cyber Security Month

Until M6, the most actively used channels have been Twitter, Facebook, and LinkedIn. Once there will be more visual and audio-visual contents produced within the project, YouTube and Instagram could also be included in the actively used channels. However, taking into account the efforts it takes to produce and customise contents for various channels and to analyse their success and impact, the choice was made to limit the number of channels, while focusing our efforts to excelling in the use of the chosen ones.

Next step is to investigate the possibility to use a social media management tool for multiple channels, such as Hootsuite, which could facilitate the planning of social media posts, as well as provide a more detailed level of analytics, to adjust our actions and maximise our reach as the project progresses.

2.9.4 Newsletter mailing list

The process of setting up the mailing list for sending out newsletters and updates to the subscribers is ongoing.

The chosen tool for creating a mailing list is Mailman. It is an open source tool and adheres to the values of the project. Most of the commonly used tools, such as MailChimp, have great potential from the marketing perspective, integrated tools for monitoring subscribers and outgoing messages, as well as predefined newsletter templates. However, these tools require a strong integration into a website, which we want to avoid. Furthermore, all the data is saved to the servers of the providers of these tools, and therefore we do not have control over it. Mailman, on the other hand, is completely self-hosted and running on servers in Switzerland that we can control.

Mailman covers our needs of sending out updates to our subscribers, allowing users to subscribe to and unsubscribe, and allows a subscription form to be integrated to the GEIGER website. To compensate for the lack of detailed analytics, A/B testing, and other tools that would be beneficial for evaluating the impact of the newsletter mailings, we can secure the personal data and the safety of our website and the mailing list, which has been considered a priority in the context of the project.

2.9.5 Events

Due to the COVID-19 crisis, all the events during M1-M6 of the project were organised online or as hybrid events, with a small group of participants physically at the venue, and the rest of them connected remotely.

2.9.5.1 Kick-off

The GEIGER project kick-off, initially planned as a two-day physical meeting, took place as a full-day video conference on 3 June 2020, entirely online. It was organised by the project lead FHNW.

The goals of the kick-off were to give an overview of the background and the preparations of the project to date, and to introduce the consortium members to each other. During the total of nearly eight-hour video conference, the project lead FHNW presented the objectives, as well as integrated technical, data science, and educational approaches, and critical success factors of the GEIGER project. The key areas of the project management, project governance, and technical work were introduced through the work packages by each work package lead. The first general assembly of the project also took place during the kick-off, and the actions points to swiftly kick-start the GEIGER project were listed for each participant.



Figure 10: GEIGER virtual kick-off and announcement of the project launch in Twitter

2.9.5.2 Pilot use case kick-off workshops

The workshops to kick-off the three pilot use cases of the GEIGER project, in Switzerland, Romania, and the Netherlands, took place during the first five months of the project. They gathered the participating consortium members to discuss the requirements and goals of the use cases, but also initiated an impressive range of contacts with third party contributors and audiences, such as MSE and start-up networks, CERTs, security experts, and potential future Security Defenders. The outcomes of these workshops are described in detail in D1.1 Requirements.

2.9.5.2.1 Swiss use case workshops

The workshop to kick-off the Swiss pilot use case took place on 24 August 2020 in Baden, Switzerland, and remote participation was also made possible by live streaming of the presentations and sessions during the first part of the workshop. The workshop was jointly organised by BBB Berufsfachschule Baden and FHNW.

The event focused on collecting stakeholder viewpoints and mapping the cybersecurity challenges and opportunities for small businesses. The exchanges with a number of local and European

stakeholders, among which the Swiss National Cyber Security Centre (NCSC) and Swiss hairdressers' association Coiffure Suisse.

The second part of the workshop introduced the concept of Reverse Education in the context of the GEIGER project. The afternoon sessions focused on designing a prototypical experience of GEIGER education, "Journey of a Certified Security Defender".

The key developments of the workshop were [live-tweeted](#) as a thread through GEIGER Twitter account, and shared in real time through [Facebook](#) and [LinkedIn](#).



Figure 11: Swiss pilot use case workshop, the first in the series of the three GEIGER pilot kick-offs

In addition to the pilot use case kick-off, more targeted workshops were organised to collect the specific input of certain stakeholders. One of these was a workshop on 25 August 2020, to discuss with [e-abo](#), [Yoga & Ayurveda Amriswil](#), and [Swiss Yoga Association](#) how cybersecurity could be made more accessible to independent entrepreneurs, particularly for entrepreneurs running yoga studios.

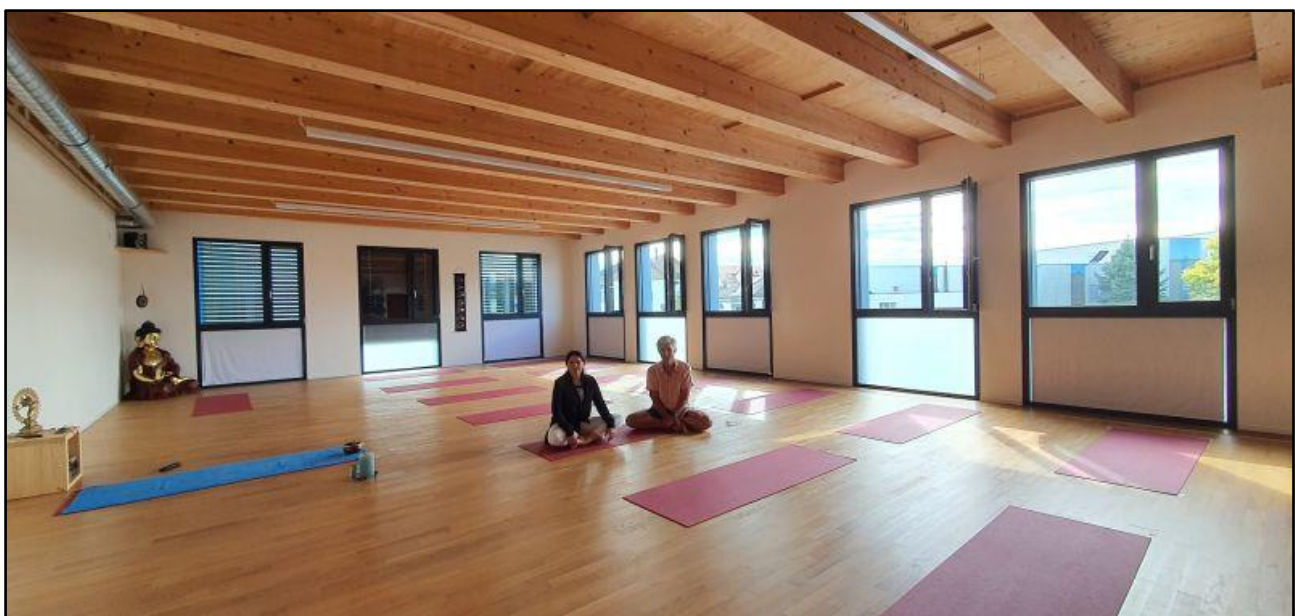


Figure 12: Workshop in August 2020 to discuss how cybersecurity could be made more accessible to entrepreneurs running yoga studios

2.9.5.2.2 Romanian use case kick-off workshop

The kick-off event for the Romanian pilot use case was organised in Cluj Napoca, Romania on 17 September, under the title 'Cyber Security: Current Practices and Priorities for SMEs', and gathered together the participating consortium members, as well as academics, representatives of small businesses, and technical experts contributing to the mapping of the landscape and priorities. Remote participation was made possible by the live-streaming of the morning session. The second

part of the workshop gathered 15 stakeholders around a roundtable to discuss different aspects of the project and the requirements and design of the GEIGER toolbox.

The key developments of the workshop were [live-tweeted](#) as a thread through GEIGER Twitter account, and shared in real time through [Facebook](#) and [LinkedIn](#).



Figure 13: Romanian pilot use case workshop, organised as a hybrid event

2.9.5.2.3 Dutch use case kick-off workshop

The Dutch pilot use case kick-off workshop took place on 1 October 2020, entirely online due to the COVID-19 situation. The objectives for the meeting were to exchange knowledge about the Dutch market, both of MSE and accountancy, to determine basic requirements and the main target group for the pilot use case, and to plan the next steps and milestones. A number of external stakeholders, including the [Digital Trust Center](#) and security experts involved in cybersecurity training, participated in the workshop

The key developments of the workshop were [live-tweeted](#) as a thread through GEIGER Twitter account, and shared in real time through [Facebook](#) and [LinkedIn](#).

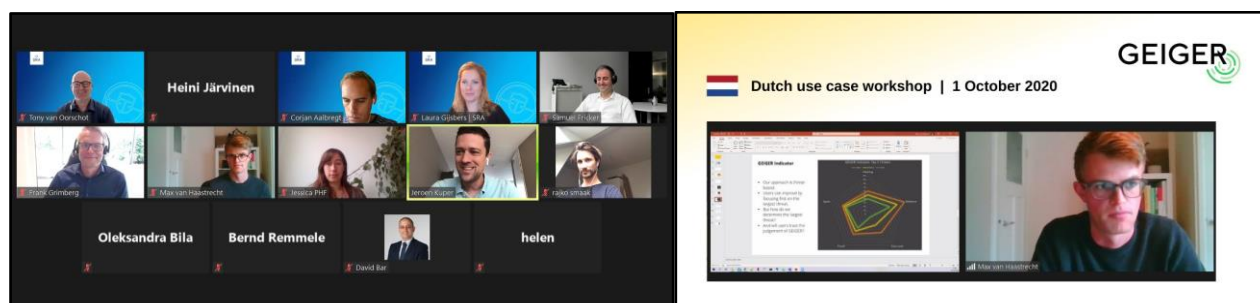


Figure 14: Dutch pilot use case workshop, organised entirely online

2.9.5.3 Cluj Innovation Days panel discussion

The first collaboration to promote the project in an event took place in a format of a panel discussion during the [Cluj Innovation Days](#), an online conference co-organised by ClujIT on 12-14 October 2020. Under the title “Reshaping work. Consolidating resilience”, it focused on overcoming today’s challenges of work in terms of tech, business and innovation. GEIGER project collaborated with the organisers of the event and coordinated a panel which discussed the increasing of the digital resilience of small businesses and presented the GEIGER project. The speakers of the panel were primarily from the GEIGER project consortium, and the debate was aimed at raising the audience's interest towards cybersecurity issues and offered a starting point to address these problems. The GEIGER project also hosted an interactive virtual expo booth on the event platform, to distribute information on the project and to interact with the event participants. Encouraged by the positive experience on this collaboration, we intend to, as part of our dissemination and communication strategy, establish similar collaborations with organisers of upcoming events relevant to our

audiences, as well as develop the concept of the virtual GEIGER expo booth, and complement it with further audio-visual presentations, to maximise its potential.

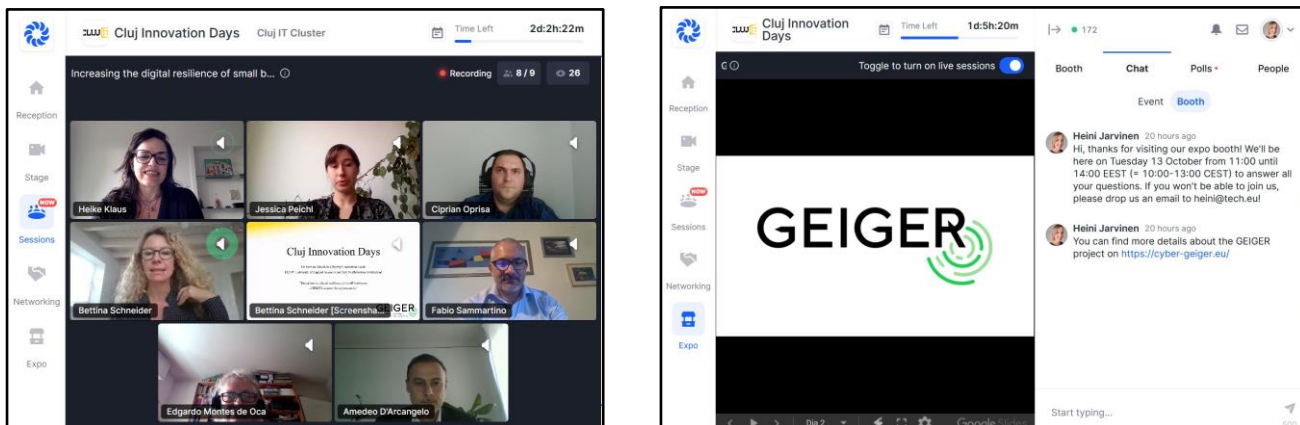


Figure 15: GEIGER panel and virtual expo booth at the Cluj Innovation Days

2.9.5.4 Participation in other events

From 31 August until 4 September 2020, in Zurich Switzerland, a GEIGER team participated in the [RE Cares Requirements Engineering conference](#) on employing RE techniques and a hackathon.



Figure 16: GEIGER team at the RE Cares Requirements Engineering conference

The GEIGER project was also presented in a lightning talk by Max van Haastrecht from UU, during the Cyberwatching.eu webinar '[Cybersecurity risk management: How to strengthen resilience and adapt in 2021](#)' on 23 November 2020, at the [Sibiu Innovation Days](#) on 26 November 2020, in a panel discussion 'Supporting the digital transformation of small businesses - cyberGEIGER counter for cybersecurity' by Jose Francisco Ruiz from Atos, and included in the topics of the workshop 'Creative Explorations – Facilitating Risk Workshops Using LEGO Serious Play' at the [Risk-!n conference](#) on 26 November 2020 by Petra Maria Asprien and Frank Grimberg from FHNW.

2.9.6 Mass media

The first [joint press release for the GEIGER project](#) was drafted for the occasion of the launch of the project. The goal of the press release was to initiate the contacts with the most relevant journalists for the success of the project, and to bring GEIGER to their attention - this is a critical part of the project's media strategy, which aims at close cooperation with selected media outlets that are most likely to be able to help us reach our primary target audience. The launch press release draft was shared as a template with the consortium and sent out by several partners to their press and media contacts, which resulted in a number of press mentions and leads for interviews.

2.9.7 Promotional and information materials

During the first six months of the project, the need for printed materials to support introducing GEIGER to our stakeholders during events and meetings was not pressing, due to the COVID-19 restrictions and the consequent lack of physical events.

2.9.7.1 Flyer

Despite that, the drafting of a flyer to present the key ideas of the project was initiated on M3 and finalised at the end of M6. The flyer is intended to be printed in A6 size, pictures a simplified graphic presentation of a mobile device screen as a background, and visually follows the GEIGER style guidelines. The front side includes a short description of the GEIGER tool, the problem it aims at solving, and its advantages, a visual representation of the GEIGER Indicator, a link and a QR code pointing to the project website and a reference to the Twitter account of the project. The back side includes the descriptions of the project, its goals, and the project consortium, consortium member logos, the key facts of the project, contact details of the project lead and media contact, and the funding acknowledgement. The flyer can be printed locally by each partner, and the design is available for all consortium members in the shared Canva visuals folder (see 'Internal organisation of communications work') in a format in which it can be edited and customised. The flyer is also

available on the file sharing platform of the project, NextCloud, and can be distributed through digital channels in PDF format.



Figure 17: Draft of the GEIGER introduction flyer

2.9.7.2 Roll-up

To increase the visibility of the GEIGER visual style, and to work towards a higher brand recognition, we drafted a GEIGER roll-up. It is of the size 80x200cm, and includes the GEIGER logo, green colour gradients defined in the style guidelines, the preliminary tagline summarising the vision of the project (see 'What: Key messages'), the consortium members' logos, website URL and Twitter handle, and the funding acknowledgement. Each partner is encouraged to get the roll-up printed locally, and use it in both physical events, and on the background of video conferences and online meetings.



Figure 18: GEIGER roll-up

2.9.7.3 Branded giveaways

Possibility to produce promotional gifts and give-aways with GEIGER branding has been discussed within the WP5 working group, and branded webcam covers has been suggested as a type of a promotional gift that would both support the vision of the project and encourage in a very concrete manner the use of privacy-enhancing tools, and act as a potential conversation starter about privacy and cybersecurity. In a situation in which the occasions to distribute promotional gifts in physical

events is limited, the compact and light format of the webcam covers will allow easy distribution also by post, if needed. It also makes it possible to produce them in a centralised way, and send out to consortium partners for distribution. The process to select the provider of these giveaways is ongoing.

2.9.7.4 Partner publications

The dissemination lead Tech.eu published on its website (70 000 viewers) two articles to introduce the GEIGER project, and to promote the project's participation in European Cybersecurity Month: '[GEIGER empowers small businesses to manage cyber threats](#)' and '[It's #CyberSecMonth! Let's talk about how to increase the digital resilience of small businesses](#)'. They were promoted through Tech.eu social media channels (50 000 followers) and newsletter (11 000 subscribers).

The project lead FHNW sent out a press release in the occasion of the project launch, and published an article '[GEIGER aims at protecting small businesses against cyber threats](#)' on their website.

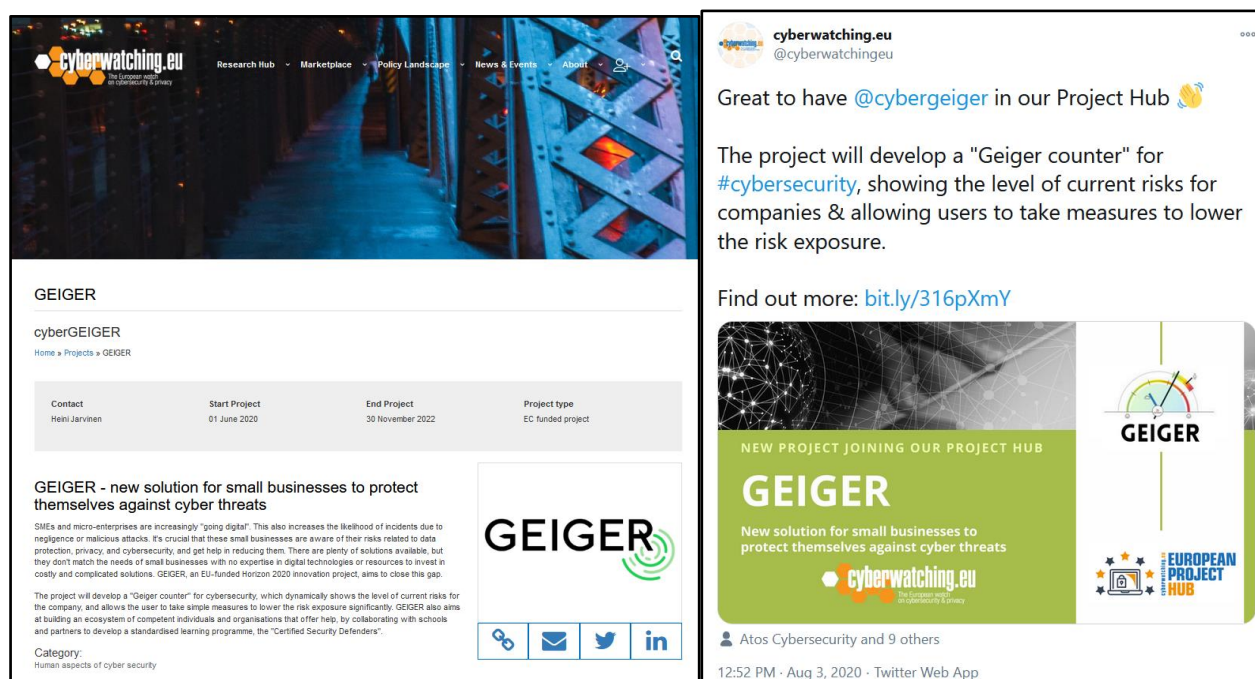
Kaspersky send out a press release '[Nasce GEIGER, un progetto innovativo promosso dalla Commissione Europea per proteggere le piccole imprese dalle minacce informatiche](#)', and published it on their website. This resulted in over 20 media mentions in the Italian online newspapers and magazines, and lead into further interviews around the project, published for example in Tom's Hardware '[Geiger: Kaspersky partecipa al progetto che mette la sicurezza informatica a portata di PMI](#)' and trade magazine Stampi '[Formazione e gamification attenti a queste due](#)'.

The first scientific publication related to the project, '[SMEs Confidentiality Concerns for Security Information Sharing](#)' by Alireza Shojaifar and Samuel A. Fricker from FHNW, was presented during the IFIP International Symposium on Human Aspects of Information Security & Assurance ([HAISA 2020](#)) on 13 July 2020.

2.9.7.5 Connecting with multipliers

As the collaboration with multipliers constitutes the backbone of the GEIGER dissemination strategy, we have started to initiate the contacts and build relations with them.

We initiated the collaboration with Cyberwatching.eu, and GEIGER is now listed on their Project Hub.



The image shows two side-by-side screenshots. The left screenshot is a project page for GEIGER on the cyberwatching.eu website. The right screenshot is a tweet from @cyberwatchingeu.

Project Page (Left):

- Header: cyberwatching.eu
- Navigation: Research Hub, Marketplace, Policy Landscape, News & Events, About
- Project Title: GEIGER
- Subtitle: cyberGEIGER
- Home » Projects » GEIGER
- Contact: Heini Järvinen
- Start Project: 01 June 2020
- End Project: 30 November 2022
- Project type: EC funded project
- Text: "GEIGER - new solution for small businesses to protect themselves against cyber threats. SMEs and micro-enterprises are increasingly 'going digital'. This also increases the likelihood of incidents due to negligence or malicious attacks. It's crucial that these small businesses are aware of their risks related to data protection, privacy, and cybersecurity, and get help in reducing them. There are plenty of solutions available, but they don't match the needs of small businesses with no expertise in digital technologies or resources to invest in costly and complicated solutions. GEIGER, an EU-funded Horizon 2020 innovation project, aims to close this gap."
- Text: "The project will develop a 'Geiger counter' for cybersecurity, which dynamically shows the level of current risks for the company, and allows the user to take simple measures to lower the risk exposure significantly. GEIGER also aims at building an ecosystem of competent individuals and organizations that offer help, by collaborating with schools and partners to develop a standardised learning programme, the 'Certified Security Defenders'."
- Category: Human aspects of cyber security
- GEIGER logo
- Social media icons: LinkedIn, Twitter, Facebook, Email

Tweet (Right):

- Profile: cyberwatching.eu (@cyberwatchingeu)
- Text: "Great to have @cybergeiger in our Project Hub 🙌"
- Text: "The project will develop a 'Geiger counter' for #cybersecurity, showing the level of current risks for companies & allowing users to take measures to lower the risk exposure."
- Text: "Find out more: bit.ly/316pXmY"
- Image: Project Hub announcement graphic with GEIGER logo and "NEW PROJECT JOINING OUR PROJECT HUB" text.
- Text: "Atos Cybersecurity and 9 others"
- Timestamp: 12:52 PM · Aug 3, 2020 · Twitter Web App

Figure 19: GEIGER listing on the Cyberwatching.eu Project Hub

To gain some additional visibility to the Cluj Innovation Days panel discussion around GEIGER and the digital resilience of small businesses, the panel was listed on the website of the [European Cyber Security Month](#).



Figure 20: The Cluj Innovation Days panel discussion around GEIGER and the digital resilience of small businesses was listed on the website of the European Cyber Security Month

2.9.8 Overview of dissemination and communications activities

The table below gives an overview of the total number of the dissemination and communication activities linked to the GEIGER project by the consortium partners.

Type of dissemination/communication activity	Total number
Organisation of a conference	4
Organisation of a workshop	3
Press Release	3
Non-scientific and non-peer-reviewed publication (popularised publication)	8
Exhibition	1
Flyer	1
Training	-
Social media (posts linked to GEIGER, throughout all channels by all consortium partners)	149
Website (articles and event reports published)	10
Communication campaign (radio, TV, social media)	1
Participation to a conference (as a speaker)	7
Participation to a workshop (presenting or linked to GEIGER)	-

Table 8: Dissemination and communication activities M1-M6

2.10 Impact tracking

To evaluate the success of the dissemination and communications efforts of the GEIGER project, we will throughout the duration of the project track the numbers indicating our progress towards the listed KPIs, and evaluate whether our efforts in each area have been successful and sufficient.

The goals and desired impact linked to gaining the attention of small business owners and staff and raising interest among them (KPIs I2.1.1.1 and I2.1.2.4) will be tracked through the numbers of impressions in social media, mass media, and targeted media, as well as (estimated or confirmed) engagement rate related to them.

As the primary target audience of the project is geographically scattered around Europe, the success of the dissemination and communications actions of the project rely to a great degree on the efforts of each consortium member. To monitor and evaluate the impact of the communications actions of all the consortium members, we set up shared spreadsheets to collect the data of all social media posts, events (participation and organising), and publications (digital and print) that have been done, as well as media mentions of the project. We also created another shared spreadsheet to collect the details on the future actions, such as events and publications, that will be used for planning our upcoming communications actions, and to make informed choices regarding the priority contents for the communications of the project for each given point of time. The consortium members are encouraged to fill in the details on their dissemination actions on a regular basis, which will allow the dissemination lead to analyse the reach and success of the coordinated efforts and make adjustments accordingly.

We will analyse the reach and engagement via the social media channels specifically created for the GEIGER project. This is currently (M6) done through the native analytics tools of each channel, such as Twitter Analytics and Facebook Insights. However, as we are investigating the possibility to use a social media management tool for multiple channels, to optimise the use of those channels, we also take into consideration the possibilities such a tool would offer for a better overview and more detailed level of analytics.

The number of subscribers to the newsletter mailings will be one of the tools to track the level of engagement and registered interest towards GEIGER. The website traffic on the GEIGER site – ideally, traffic sources (organic, referral, direct, social), bounce rate, top pages, and conversion rate – will be also measured, to analyse and adjust the publications on the website, as well as their promotion. As the project website is, and the mailing list will be built with the special focus on data protection and digital security, the potential tools to analyse the traffic in a manner that respects the privacy of the site visitors and handles the data in a way that complies to the highest data protection standards is being explored and discussed.

The impact of the press work and actions will be mainly evaluated through the number of media mentions and their reach, which are tracked through the monitoring work done by the dissemination lead, as well as the mentions the consortium members list in the shared tracking sheet. When evaluating the impact of these media mentions, the relevance of the media outlet to our primary target audience must be taken into account.

To track the number of stakeholders who have confirmed their intent to recommend or adopt GEIGER (KPIs I2.1.4.3, I2.1.4.4, I2.1.4.5, I2.1.1.6, I2.1.1.7, I2.1.1.8) we will seek to secure their letters of intent, and this will be used as a clear indicator of the achieved impact.

The numbers indicating how many MSEs installed and tested the GEIGER toolbox and benefited from the Security Defenders' support will be used for tracking the perhaps most critical goal of the project – having successfully reached the primary target audience and convinced them to try GEIGER (KPI I2.1.1.2).

2.10.1 Risk management

The general risks related to reaching the KPIs of the T5.1 include a failure to define reliable ways of measuring the progress towards the KPIs, lack of communication or consensus within the consortium, delays in the work of other tasks or work packages that have an impact on T5.1, key members of the work package or project leaving the GEIGER project, and insufficient communications efforts by consortium partner or third party collaborators to create the desired impact. These risks can be, in general, mitigated by close collaboration between the consortium partners in defining the best practices, allowing open feedback and corrective actions, and keeping each other up to date on the status of their work.

The following table points out the most likely risks related to the key KPIs of T5.1, and suggested action to mitigate these risks:

KPI	Stage of the project	% of KPI reached (estim.)	Key actions towards achieving the KPI	Risk	Mitigation
I2.1.4.1 ≥1'000'000 impressions of the GEIGER Indicator as measured by number of impressions of media channels	M1-M6	5%	1) Mass media impressions 2) Targeted media impressions 3) Social media impressions (via GEIGER and partner channels) 4) Impressions in events (consortium partners' participation as speakers)	Failure to activate all consortium partners.	Collecting feedback regarding internal collaboration and adjusting practices. Simplifying processes to allow easy participation.
	M7 - M18	20%		Insufficient outreach towards networks of multipliers by consortium partners.	Reinforcing the internal collaboration within the consortium. Developing ready-to-distribute introduction materials for consortium partners
	M19 - M24	35%		Failure to activate the networks of multipliers.	Developing ready-to-distribute campaigns or publications for consortium partners to offer to the identified multipliers.
	M25 - M30	50%		Lack of or low visibility in mass media and via multiplier channels.	Early contacts with press/multipliers. Preparing suitable communications materials according to the formats and style of the desired key channels.
I2.1.1.1 >500'000 SMEs&MEs will be aware	M7 - M18	25%	1) Encouraging newsletter mailing list subscriptions	Low number of subscriptions or	Testing, evaluating, and adjusting the messaging for each target audience, in
	M19 - M24	35%			

of the GEIGER Indicator as a dynamic risk monitoring instrument	M25 - M30	40%	2) Social media promotion to grow follower base & create engagements 3) Facilitating registration of interest in events	engagement due to inefficient messaging. Insufficient amount of direct interactions and participation in discussions via social media. Wrongly chosen focus channels.	cooperation with consortium partners and third parties (e.g. key multipliers). Increasing the efforts to create direct connections to multiplier organisations and influential individuals via social media. Analysing the efficiency of the used channels and focusing efforts to those bringing the best results.
I2.1.2.4 ≥100'000 small enterprises have a GEIGER account, allowing them to predict their risk with the personalised GEIGER Indicator and benefit from the GEIGER toolbox.	M19 - M24	40%	1) Integration of an easy procedure to create a GEIGER account to the GEIGER website 2) Targeted CTA communications towards subscribers and followers	Delays in the development of the GEIGER Solution → Lack of the platform where to create a GEIGER account. Inefficient messaging to activate the primary target audience.	Close collaboration with the consortium partners involved in the technical development of GEIGER Solution. Evaluating and adjusting the messaging for each target audience, in cooperation with consortium partners and third parties (e.g. key multipliers).
	M25 - M30	60%			

I2.1.1.2 >50'000 SMEs&MEs will have tried the personalised GEIGER Indicator for their own specific SME&ME by registering on GEIGER Solution	M19 – M24	20%	1) Communication s through all channels to familiarise the potential end users with the GEIGER interface and functionalities 2) Targeted training & workshops on the use of the GEIGER tools	Delays in developing the GEIGER Solution → No platform to try the GEIGER Indicator. Confusing or irrelevant features, or low ease-of- use of the developed GEIGER Solution.	Close collaboration with the consortium partners involved in the technical development of GEIGER Solution and its interface.
	M25 – M30	80%			

Table 9: Most likely risks related to the key KPIs of T5.1 and suggested actions to mitigate them

2.11 Summary and Conclusions

This section gave an overview of the dissemination and communications plan for the GEIGER project. It also listed the achievements, actions completed, and communications materials produced during the first six months of the project.

The key take-aways of this strategy for GEIGER dissemination and communications and the building of the ecosystems of MSEs and "Security Defenders", are:

- 1) aiming, systematically and from an early stage of the project on, at creating connections to multiplier networks that will allow us to reach our primary target audiences;
- 2) close collaboration within the consortium and with the identified external multipliers to work on framing and messaging that appeal to our target audiences, and to plan communications actions and materials that efficiently reach them, and
- 3) continuous tracking of the progress towards our objectives, as well as evaluating the success of the chosen methods and actions and adjusting them to reach the maximum impact.

3 T5.2 Standardisation and Liaison with Policy

3.1 Introduction

GEIGER, consisting of the GEIGER technical framework and the GEIGER Security Defenders education, is intended to be a solution that is open to related activities within Europe and worldwide. With openness, it aims at offering maximal cybersecurity and data protection impact for micro and small enterprises (MSEs). Openness is intended to be achieved through harmonisation and mutual recognition of external interfaces with third parties and in liaison with relevant standardisation.

The GEIGER solution will enable an ecosystem consisting of MSEs that includes their staff as human end-users, cybersecurity and education tool developers, CERTs competent for the MSEs, educators, and human certifiers. For each such ecosystem player, interfaces will be created, allowing the exchange of data and results. The following context diagram gives an overview of the interfaces that will be offered by GEIGER to tools, CERTs, Educators and Certifiers, and MSEs.

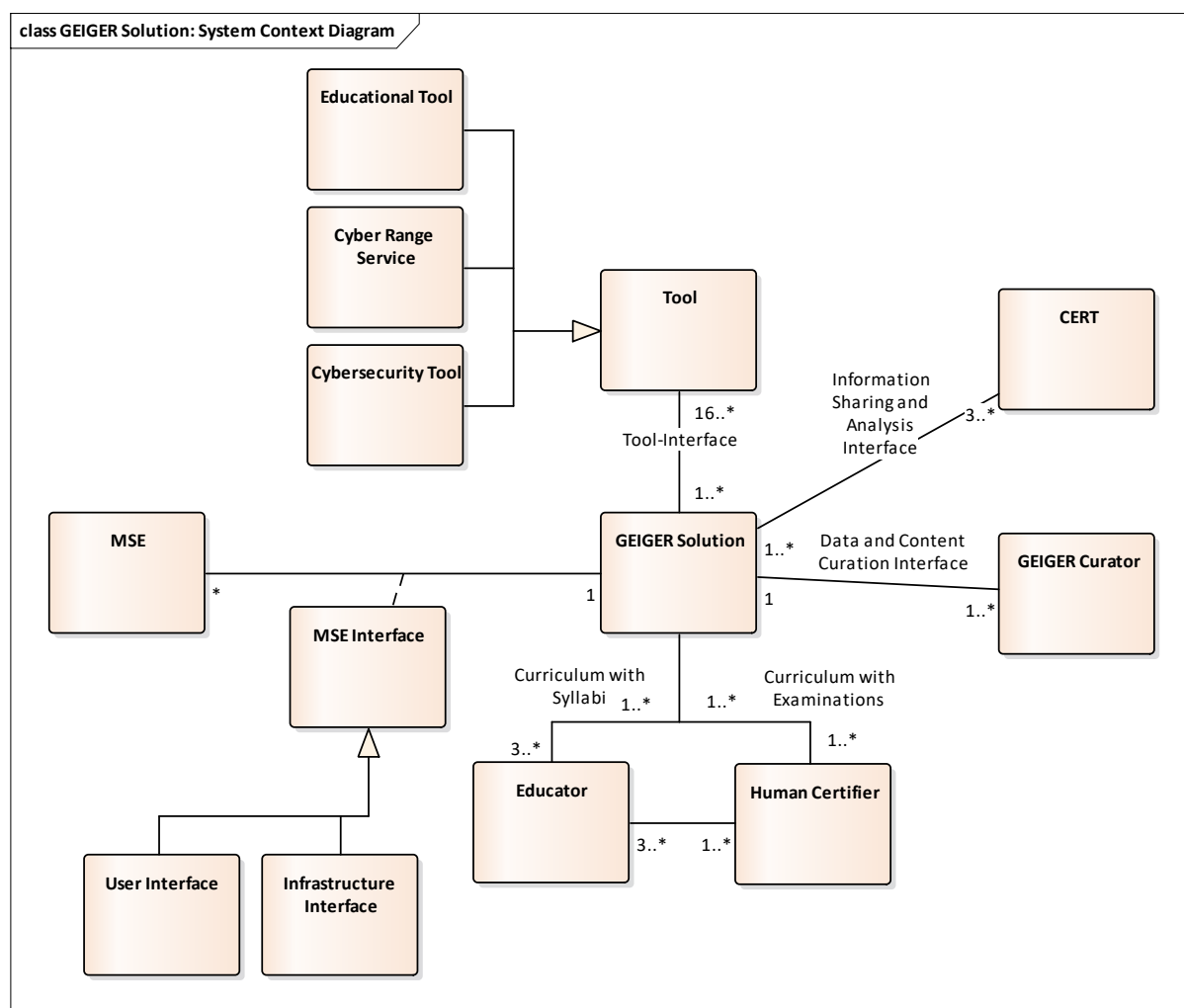


Figure 21: Position existing maps and landscapes

Within the Tasks T1.1, GEIGER analysed the critical needs of stakeholders in the GEIGER ecosystem. Three complementary strategies will be pursued to enable the satisfaction of these needs:

- A. Implementation of capabilities in the GEIGER solution that match these needs. The technical GEIGER framework will be implemented in WP2 and the Security Defenders education in WP3. Validation will take place in WP4.

- B. Enable matchmaking with a competent third-party member of the GEIGER ecosystem through a GEIGER-defined interface. These interfaces will be implemented and tested in WP2 and WP3 and validated in WP4.
- C. Liaison with standardisation and policy definition enabling interoperability with a large number of potentially diverse third parties. WP5 has identified standards and policies for guiding the implementation of the GEIGER solution and will contribute with recommendations for the evolution of standards and policy based on lessons learned. To enable liaison, GEIGER will initiate a dialogue with relevant stakeholders.

In line with the descriptions provided by the GA, the contributions from the GEIGER project will include (C1) the Security Defenders curriculum, (C2) an open API for interoperability with security, cyber range, and educational tools for MSEs, (C3) an open API for information sharing and analysis, and (C4) recommendations for policy definition enhancing the protection of MSEs. The following table gives an overview and connects these planned results with the KPIs defined in Annex 1 of the GEIGER Grant Agreement (GA).

KPI	Target defined in GA	Planned Contributions
I2.1.2.8	1 open API with API access governance policies for querying incidents and submitting information	(C3): 1 open API for information sharing and analysis. The API will be used for data exchange between the GEIGER Framework and the CERTs competent for the MSEs who the data subjects are and have given consent to the information sharing.
KPI 3.2	4 open APIs allowing connectivity with MSEs, SME associations, and CERTs/CSIRTs, and third-party tool and framework providers.	<p>The refined understanding of the GEIGER ecosystem and GEIGER framework architecture resulting from requirements analysis and reported in D1.1 leads to the following plan for achieving the KPI 3.2:</p> <p>(C1 – 1 open API): the curriculum with matching syllabus recommendations and examination will be encoded and made available for used by SCORM-based learning management systems.</p> <p>(C2 – 2 open APIs): in the refined GEIGER Toolbox, at least the following types of tools will be integrated with their respective API specialisation: educational tools (API based on xAPI and SCORM as applicable) as well as sensor, shield, and recommender tools (API based on MISP as applicable).</p> <p>(C3 – 1 open API): information sharing and analysis with CERTs based on MISP.</p>

I2.1.2.9	4 contributions to standardisation work or memorandums of understanding with related initiatives for harmonising external GEIGER interfaces.	The contributions will be associated with the following planned GEIGER results. (C1): 1 curriculum with matching syllabus recommendations and examination for Certified Security Defenders Education. (C2): 1 open API for interoperability with cybersecurity, cyber range, and education tools, enabling the integration of these tools in the GEIGER Toolbox. (C3): 1 open API for information sharing and analysis with CERTs competent for the MSEs who the data subjects are and have given consent to the information sharing. (C4): 1 recommendation for policy definition concerning the protection of small businesses depending on third-party social networks and clouds.
I2.1.4.7	≥2 contributions to standardisation.	See planned contributions for I2.1.2.9 (C1, C2, and C3).

Table 10: Key KPIs for T5.2

Several maps have been developed that give an overview of cybersecurity-related standardisation efforts. For example, the project Cyber Security for Europe has published a map of standards and standardisation projects⁶ of the standards-defining organisations (SDO) CEN/CENELEC, ISO, ETSI, ITU, IETF, and other national SDOs⁷. Even though the effort in the standardisation of cybersecurity for SMEs is growing⁸, no map has been published with a clear focus on security and data protection for small businesses, however.

This section fills this gap with a specialised investigation of standards and regulations that are relevant from the perspective of the GEIGER partners for guiding the GEIGER work on bringing cybersecurity to MSEs. The investigation has been performed with a structured questionnaire answered by the 18 GEIGER consortium partners, many of which are involved in relevant standards-defining initiatives and organisations. The result and contribution of this section is a comprehensive map of standards and their associated organisations that is useful for guiding the implementation of relevant aspects of the standards in WP2 and WP3 and for liaison with relevant initiatives and SDOs for the planned contributions.

The remainder of this section is structured as follows. The subsection Methodology describes our standards mapping approach. The subsection Standards and Regulation and the subsection Standardisation and Policy-Definition Initiatives offer the results identified in the mapping. The section Selection of Standards and Regulations offers recommendations for the consideration of standards in WP2 and WP3. The section Expected Contributions to Standards and Policy outlines the planned contributions to standardisation work and policy definition. The section Summary and Conclusions summarises the contribution of this section and outlines how future work in GEIGER will build on the contribution.

⁶ Cyber Security for Europe, D8.2 Project Standards Matrix, July 20, 2020. <https://cybersec4europe.eu/wp-content/uploads/2020/09/CS4E-D8.2-Project-Standards-Matrix-v1.1.pdf>

⁷ Cyber Security for Europe, D8.1 Cybersecurity Standardization Engagement Plan, August 5, 2019. https://cybersec4europe.eu/wp-content/uploads/2019/11/CS4E-Deliverable-D8.1_v2.1_2019_08_05_final.pdf

⁸ B. Ozkan, M. Spruit, “Cybersecurity Standardisation for SMEs: The Stakeholders’ Perspectives and a Research Agenda”, *International Journal of Standardization Research* 17(2):41-72.

3.2 Methodology

During the months M1-M6, T5.1 aimed to make explicit organisations and initiatives related to standardisation and policy definition activities and with relevance to GEIGER. With the awareness of these standards, organisations, and initiatives, the T1.2, T1.3, and T1.4 teams have the necessary decision-support for positioning of GEIGER and the definition of the GEIGER framework architecture, indicator, and education.

A questionnaire-based approach was used to perform the mapping involving the whole GEIGER consortium. The map was intended to answer the mapping questions MQ1 *What standards and ongoing standards-defining organisations and initiatives are related to cybersecurity for MSEs?* MQ2 *What policies and ongoing policy-defining organisations (SDOs) and initiatives are related to cybersecurity for small businesses?* MQ3 *In what standards or policy-defining organisations or initiatives are the GEIGER partners involved?* The answers to the first two mapping questions allowed the consortium to become aware of potentially relevant standards and policies and select those that should be considered in the GEIGER project. The answer to the third mapping question was used to plan for liaison with the relevant SDOs or initiatives for contributing to standardisation, respectively policy-definition.

The involvement of the 18 GEIGER consortium partners was deemed suitable for the following reasons. The consortium partners comprise end-user organisations seeing relevant market offerings, technology experts with a good overview of ongoing innovations, and competent universities involved in the scientific dialogue about cybersecurity for small businesses. Their knowledge was useful for identifying relevant organisations and initiatives. The consortium partners' involvement in these organisations and initiatives will be useful for initiating the dialogue for contributions to selected organisations and initiatives. The map was complemented with input from the project officer sharing the European Commission's view of projects and initiatives. The following table gives an overview of the involved partners.

Perspective	Expert Organisations
End-users	SKV, HAAKO, E-ABO, SCB, PT, CL
Technology	ATOS, FHNW, KASP, MI, KPMG, CLUJ IT
Education	PHF, FHNW, BBB, CLUJ IT, SRA
Science	UU, FHNW, PHF
Policy	TECH.EU, CERT-RO, SRA, European Commission

Table 11: Overview of the involved partners

The questionnaire summarised in the following table was prepared to collect the inputs from these partner organisations. The questionnaire was completed during the months M2-M5 of the GEIGER project. Three meetings were held to inform the partners about the mapping activities, offer clarifications, and share the results.

Section	Requested Inputs
1. Partner's background	Experience in cybersecurity standardisation Standards-definition organisations with partner involvement Contact persons
2. Previous and ongoing work	Already published maps Related projects
3. Organisations and initiatives	Standardisation-related events Standardisation organisations and workgroups Visions and roadmaps influencing standardisation
4. Standards and regulations	Classification of SMEs Threat, risk, and response modelling or assessment Data protection and privacy Data exchange and information sharing Education
5. Conclusions	Comments and suggestions

Table 12: Requested inputs

The mapping questions MQ1-2 were answered by analysing the content of the answers given for sections 2-5, the mapping question MQ3 by analysing the answers given for section 1. Content analysis was performed by aggregating the answers into categories and using the affected GEIGER component or external interface as a criterion for the grouping. The resulting map was checked by the GEIGER consortium members for correctness and completeness.

The map offers a useful overview of ongoing standardisation and policy definition efforts. Its contents are actionable thanks to the clear links to GEIGER components and the relations of GEIGER partners with the standardisation and policy definition. At the same time, the map has limitations. It reflects only the knowledge of the GEIGER consortium. Keyword-based database and internet searches as well as checking by competent third parties would be useful to extend the map further.

3.3 Organisations and Initiatives

This sub-section lists activities of standards-related organisations and projects that are of relevance for GEIGER.

3.3.1 Standardisation

The following table gives an overview of standards-defining organisations together with their activities that are of relevance for GEIGER according to the consortium members' opinion. The table indicates the relevance of the activities in terms of the scope of applicability in GEIGER. It also shows the GEIGER partners that are involved in the respective activity.

Organisation	Activities	Relevance	Partners
ISO/IEC JTC 1/SC 27	ISO/IEC work programme on information security, cybersecurity and privacy protection		
	WG1 Information security management systems	GEIGER Method	ATOS

	WG3 Security evaluation, testing and specification	GEIGER Indicator	-
	WG4 Security controls and services	GEIGER Toolbox	-
	WG5 Identity management and privacy technologies	MSE Compliance	ATOS
CEN/CLC/JTC 13	European Standards-defining organisation with 6 workgroups on cybersecurity and data protection		
	WG2 Management systems and controls sets	GEIGER Method	-
	WG3 Security evaluation and assessment	GEIGER Indicator	UU
	WG4 Cybersecurity services	GEIGER Toolbox	-
	WG5 Data protection, privacy and identity management	MSE Compliance	-
	WG6 Product security	Digital Enabler MSEs	-
ECSO	European Cyber Security Organisation		
	WG1 Standardisation, certification and supply chain management	Digital Enabler MSEs	ATOS
	WG3 Sectoral demand	GEIGER Organisation	-
	WG4 Support to SMEs (registry, EU cybersecurity label) ⁹	Start-up MSEs	-
	WG5 Education, awareness, training, cyber ranges, incl. EHR4CYBER ¹⁰	Security Defender Education	-
	WG6 SRIA and Cyber Security Technologies	GEIGER Project	-
ETSI TC CYBER	Technical Committee on Cyber Security with a focus on IoT		
	Work on the protection of personal data and communication	MSE Compliance	-
	Work on cybersecurity tools & guides	GEIGER Toolbox	UU
ENISA	European Union agency for cybersecurity		
	Operational cooperation, incl. CSIRTs network, incident reporting, and threat and risk management	GEIGER Indicator	-

⁹ <https://www.ecs-org.eu/documents/uploads/wg4-position-paper.pdf>

¹⁰ <https://www.ecs-org.eu/documents/publications/5bf7e01bf3ed0.pdf>

	Capacity building, incl. cybersecurity awareness and education	Security Defender Education	-
	Trusted solutions, incl. data protection and standards and certification	Digital Enabler MSEs	CERT-RO
ISACA	Organisation for advancing talent, expertise and learning in technology		
	Cybersecurity education and certificates	Security Defender Education	-
X-ISAC ¹¹	Information Sharing and Analysis Centre for other ISACs, information sharing communities, and CSIRT networks. Provides core software, cross-sector threat intelligence, taxonomies, and open standards.	GEIGER Indicator	-

Table 13: Relevance of the standardisation activities, and the involvement of GEIGER partners

The overview shown above includes standardisation work that is potentially relevant for GEIGER. Not included in the overview are SDOs like ITU-T and IETF. No work could be identified in these SDOs that has a clear focus on standards for the protection of small businesses. Also not included in this overview are regional or national initiatives. These would comprise, for example, the cybersecurity framework of Baden-Württemberg (with PHF involvement), the Spanish standards body UNE (with ATOS involvement), and the Dutch chapter of NEN (with UU involvement). Finally, not included in this overview are uses of standards for guidance and certification of organisations. For example, KPMG is guiding and certifying organisations based on ISO 27'000 and GDPR.

3.3.2 Policy Definition

The following table lists organisations influencing policy definition together with their activities that are of relevance for GEIGER. The table indicates the relevance of the activities in terms of scope of applicability in GEIGER. It also identifies the GEIGER partners that are involved in the respective activity.

Organisation	Activities	Relevance	Partners
ENISA	Cybersecurity policy, incl. NIS Directive	GEIGER Organisation	-
Swiss Government	National strategy for the protection of Switzerland against cyber risks (NCS) 2018-2022 ¹²	GEIGER Organisation	FHNW
SME Europe ¹³	Representation of SMEs for developing and advising on EU legislation for SMEs.	GEIGER Ecosystem	-

¹¹ <https://www.x-isac.org/>

¹² https://www.isb.admin.ch/isb/en/home/themen/cyber_risiken_ncs/ncs_strategie.html

¹³ <http://www.smeeurope.eu/about-us/>

European Digital SME Alliance ¹⁴	Network of ICT SMEs in Europe representing the interests of the members vis-à-vis the institutions of the European Union.	GEIGER Ecosystem	FHNW
---	---	------------------	------

Table 14: Organisations influencing policy definition, their activities that are of relevance for GEIGER, and the GEIGER partners involved

3.3.3 Related Projects

The following table lists projects that are related to GEIGER. The table indicates the relevance of the activities in terms of scope of applicability in GEIGER. It also identifies the GEIGER partners that are involved in the respective activity.

Project (Timing)	Description ¹⁵	Relevance	Partners
CyberSec4Europe (2019-02 – 2022-07)	Governance structures for a future European Cybersecurity Competence Network: https://cybersec4europe.eu/	Security Defender Education	ATOS
CyberWiser (2018-09 – 2021-02)	Cyber range-based cybersecurity training for basic and advanced beginners with a cybersecurity professionals register (CyPR ¹⁶): https://www.cyberwiser.eu/	Security Defender Education	ATOS
Concordia (2019-01 – 2022-12)	Cybersecurity competence network: https://www.concordia-h2020.eu/	GEIGER Ecosystem	ATOS
ECHO (2019-02 – 2023-01)	European network of cybersecurity centres: https://echonetwork.eu/	GEIGER Organisation	-
CyberWatching (2017-05 – 2021-07)	European observatory of research and innovation in cybersecurity and privacy: https://www.cyberwatching.eu/	GEIGER Project	-
SMESEC (2017-06 – 2020-05)	Framework for protecting small and medium-sized enterprises: https://www.smesec.eu/	GEIGER Framework	FHNW, ATOS, UU
SU-DS03 Project: CyberKit4SME (2020-06 – 2023-05)	Tools for cybersecurity and data protection risk awareness, monitoring, forecasting, and management in small businesses.	GEIGER Framework	-
SU-DS03 Project: Palantir (2020-09 – 2023-08)	Framework for privacy assurance and data protection based on incident detection and recovery.	GEIGER Toolbox	-

¹⁴ <https://www.digitalsme.eu/>

¹⁵ For the projects without linked URL, no online presence has been found.

¹⁶ <https://www.cyberwiser.eu/cypr>

SU-DS03 Project: Puzzle (2020-09 – 2023-08)	Tools for SMEs to monitor, forecast, assess, and manage cyber risks.	GEIGER Indicator	MI
SU-DS03 Project: Trapeze (2020-09 – 2023-08)	Blockchain and linked data for citizens to manage security and privacy.	-	KSP
SU-DS05 Projects: AI4HealthSec (2020-10 – 2023-09) HEIR (2020-09 – 2023-08) CityScape (2020-09 – 2023-08)	Analysis of cyberattacks and threats for situational awareness and incident handling in healthcare and transport ICT infrastructures.	GEIGER Indicator	KSP in CityScape
FORTIKA (2017-06 – 2020-05)	Hardware-enabled security middleware reusing existing third-party cybersecurity services for SMEs: https://fortika-project.eu/	Digital Enabler SMEs	-
GDPR Cluster Project: PoSelD-on (2018-05 – 2020-12)	Blockchain-based solution for safeguarding data subject rights and ensuring organisations' GDPR compliance: https://www.poseidon-h2020.eu/	Data Protection	-
Interreg Cyber (2018-06 – 2023-05)	Boost the competitiveness of European cybersecurity SMEs by creating synergies among European cybersecurity valleys: https://www.interregeurope.eu/cyber/	Digital Enabler SMEs, GEIGER Toolbox	-

Table 15: Projects related to GEIGER and GEIGER partners' involvement in them

3.4 Standards, Regulations, and Recommendations

This section offers tables that list standards, regulations, and established recommendations of relevance for GEIGER. The tables indicate the relevance of the standards and regulations in terms of the scope of applicability in GEIGER.

3.4.1 SMEs

Standard	Description	Relevance
European Commission: SME definition ¹⁷	Distinction of SME types based on their size, turnover, and balance sheet.	GEIGER Ecosystem

¹⁷ https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en

European Digital SME Alliance: position paper on EU Cybersecurity Act ¹⁸	Distinction of SME types based on their role in the digital ecosystem for tailoring cybersecurity solutions.	GEIGER Ecosystem
European Commission: Skills for SMEs ¹⁹	Roadmap for bringing cybersecurity skills to SMEs.	GEIGER Project

Table 16: SME standards, regulations, and established recommendations of relevance for GEIGER

3.4.2 Cybersecurity

Standard	Description	Relevance
ISO/IEC 27000 family of standards ²⁰	Management system form managing information security risks and controls within an organisation.	GEIGER Method
ISO 31000 family of standards ²¹	Risk management guidance for organisations.	GEIGER Indicator
NIST Cybersecurity Framework ²²	Cybersecurity activities, outcomes, and references helping a critical infrastructure organisation to align and prioritise its cybersecurity activities with business requirements, risk tolerances, and resources.	GEIGER Method
NIST Risk Management Framework ²³	A system life cycle approach for managing security and privacy risks in information systems and organisations.	GEIGER Indicator
NIST Computer Security Incident Handling Guide ²⁴	Guide for establishing computer security incident response capabilities and handling incidents efficiently and effectively.	GEIGER Incident Handling
ENISA Reference Incident Classification Taxonomy ²⁵	Reference incident classification taxonomy with mapping to related taxonomies.	GEIGER Incident Handling
MISP Taxonomies and Classification ²⁶	CERT-XLM Security Incident Classification, DFRLab Dichotomies of Disinformation, Detection Maturity Level (DML) model, and Permissible Actions Protocol for use in MISP.	GEIGER Incident Handling

¹⁸ <https://www.digitalsme.eu/digital/uploads/The-EU-Cybersecurity-Act-and-the-Role-of-Standards-for-SMEs.pdf>

¹⁹ <https://op.europa.eu/en/publication-detail/-/publication/82aa7f66-67fd-11ea-b735-01aa75ed71a1/language-en>

²⁰ <https://www.iso.org/isoiec-27001-information-security.html>

²¹ <https://www.iso.org/iso-31000-risk-management.html>

²² <https://www.nist.gov/cyberframework/framework>

²³ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf>

²⁴ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf>

²⁵ <https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy/>

²⁶ <https://www.misp-project.org/taxonomies.html>

AFM Principles for Information Security ²⁷	Set of principles for information security to ensure that firms have taken appropriate measures for continuity and reliability of information technology, information, and provision of information.	GEIGER Method
ENISA EUCC Cybersecurity Certification ²⁸	Candidate EU cybersecurity certification scheme for ICT products.	Digital Enabler MSEs
3GPP and GSMA Network Equipment Security Assurance Scheme (NESAS) ²⁹	Security requirements and assessment framework for secure product development and lifecycle processes in the mobile industry.	Digital Enabler MSEs
ETSI GS ISI 003	Key performance security indicators to evaluate the maturity of security event detection	GEIGER Indicator
ISACA: Cyber Security Check Guide	Guide for cybersecurity checks in the IT office IT of companies and government agencies	GEIGER Indicator
ICT Switzerland: Cybersecurity Quick Check for SME ³⁰	Set of self-assessment questions with associated recommendations for SMEs.	GEIGER Indicator
Cyber Security Raad: Cybersecurity Health Check ³¹	Health check for gaining insight into cybersecurity within a medium-sized enterprise.	GEIGER Indicator
NCCIC: ICS Cyber Security Evaluation Tool	Guide for evaluating industrial control system and information technology network security practices	GEIGER Indicator
German BSI: IT-Grundschutz Kompendium	Practical overview of threats, vulnerabilities, and advice for information security adapted to the current state-of-the-art ³²	GEIGER Indicator
MITRE: ATT&CK	Knowledge base of adversary tactics and techniques for the development of threat models and protection methodologies ³³	GEIGER Indicator
University of Utrecht	Method for modelling adaptive information security for SMEs in a cluster ³⁴	GEIGER Method

²⁷ <https://www.afm.nl/~/-/profmedia/files/publicaties/2019/principes-informatiebeveiliging-en.pdf?la=en>

²⁸ <https://www.enisa.europa.eu/publications/cybersecurity-certification-eucc-candidate-scheme>

²⁹ <https://www.gsma.com/security/network-equipment-security-assurance-scheme/>

³⁰ <https://ictswitzerland.ch/en/topics/cyber-security/check/>

³¹ https://www.cybersecurityraad.nl/binaries/Cybersecurity_Health_Check_ENG_tcm107-357231.pdf

³²

https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/itgrundschutzKompendium_node.html

³³ <https://attack.mitre.org/>

³⁴ <https://www.emerald.com/insight/content/doi/10.1108/JIC-05-2019-0128/full/html>

University of Utrecht	IFSAM: The Information Security Focus Area Maturity Model ³⁵	GEIGER Method
-----------------------	---	---------------

Table 17: Cybersecurity standards, regulations, and established recommendations of relevance for GEIGER

3.4.3 Data Protection and Privacy

Standard	Description	Relevance
General Data Protection Regulation (GDPR) ³⁶	Regulation 2016/679 of the EU parliament and council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.	MSEs
EDPB: Guidelines for Controllers and Processors ³⁷	Guidelines and examples for the implementation of the GDPR by controllers and processors of personal data.	MSEs
CNIL: Guides and Templates ³⁸	GDPR guide and record of processing activities to assist processors and GDPR developer's guide	MSEs, incl. Digital Enabler MSEs
Swiss Federal Act on Data Protection ³⁹	Law aiming at protecting the privacy and the fundamental rights of persons when their data is processed.	MSEs
ISO/IEC 29100 family of standards ⁴⁰	Privacy framework covering terminology, roles, privacy safeguarding considerations, and privacy principles for information technology.	GEIGER Method
NIST Privacy Framework ⁴¹	Guide for improving privacy through enterprise risk management supporting privacy-by-design concepts and help organisations protect individuals' privacy.	GEIGER Method

Table 18: Data protection and privacy standards, regulations, and established recommendations of relevance for GEIGER

3.4.4 Data Exchange and Information Sharing

Standard	Description	Relevance
MISP Information Exchange and Data Modelling ⁴²	Set of standards to support information exchange and data modelling in cybersecurity and threat intelligence and vulnerability and incident response information. Official source and several open-source platform implementations available.	GEIGER Information Sharing

³⁵ <https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1180&context=ecis2014>

³⁶ <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679>

³⁷ https://edpb.europa.eu/guidelines-relevant-controllers-and-processors_en

³⁸ <https://www.cnil.fr/en/home>

³⁹ <https://www.admin.ch/opc/en/classified-compilation/19920153/index.html>

⁴⁰ <https://www.iso.org/standard/45123.html>

⁴¹ <https://www.nist.gov/privacy-framework/privacy-framework>

⁴² <https://misp-standard.org/>

MISP Community Data Models ⁴³	Series of JSON-encoded data models based on the MISP core format created by the MISP community.	GEIGER Information Sharing
YARA Malware Classification ⁴⁴	Description of malware families based on textual or binary patterns.	-
MeliCERTes Platform ⁴⁵	The European Cyber Security Platform MeliCERTes is a network for establishing trust among the national CSIRTs of the EU member states.	-
SCORM 2004 ⁴⁶	SCORM is a set of technical standards that allow products for eLearning content and learning management systems to work together.	Security Defender Education
Experience API (xAPI) ⁴⁷	The Experience API is a specification for learning technology that makes it possible to collect data about the online and offline learning experiences of a person or group.	Security Defender Education, GEIGER Toolbox

Table 19: Data exchange and information sharing standards, regulations, and established recommendations of relevance for GEIGER

3.4.5 Education Standards and Offerings

Standard	Description	Relevance
NIST NICE Cybersecurity Workforce Framework ⁴⁸	Reference resource to support a workforce capable of meeting an organisation's cybersecurity needs.	Security Defender Profile
Swiss ICT Competence Framework ⁴⁹	Framework of modules for the education of ICT professionals in Switzerland.	Security Defender Profile
NIST Small Business Cybersecurity Corner ⁵⁰	Cybersecurity training resources for small businesses.	Security Defender Education
ACM Cybersecurity Education Framework ⁵¹	Comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity offerings at the post-secondary level.	Security Defender Education

⁴³ <https://www.misp-project.org/datamodels/#misp-core-format>

⁴⁴ <https://virustotal.github.io/yara/>

⁴⁵ <https://github.com/melicertes/>, <https://ec.europa.eu/digital-single-market/en/news/call-tender-advance-melicertes-facility-used-csirts-eu-cooperate-and-exchange-information>

⁴⁶ <https://scorm.com/>

⁴⁷ <https://xapi.com/overview/>

⁴⁸ <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf>

⁴⁹ <https://www.ict-berufsbildung.ch/berufsbildung/ict-competence-framework/>

⁵⁰ <https://www.nist.gov/itl/smallbusinesscyber>

⁵¹ <https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf>

EFF Security Education Companion ⁵²	Resource for people teaching digital security to friends and neighbours.	Security Defender Education
ISACA CSX Cybersecurity Nexus Training and Credentialing ⁵³	Cybersecurity real-world, hands-on skills training.	Security Defender Education
CompTIA Cybersecurity Certifications ⁵⁴	IT certifications from entry-level to expert: CompTIA CySA+, CASP+ and PenTest+	Security Defender Education
CISCO Security Certifications ⁵⁵	CISCO security training and certifications, incl. CyberOps Associate and Professional, CCNP Security, and CCIE Security. Connected to the CISCO Networking Academy ⁵⁶ .	Security Defender Education
Global Cyber Academy Courses ⁵⁷	UK-based business education academy with courses on cybersecurity and GDPR.	Security Defender Education
Quality Assurance for CyberSec4Europe MOOCs ⁵⁸	Quality assurance process and criteria for massive open online courses (MOOCs) in Europe in the form of academic, continuous learning, and cyber range courses.	Security Defender Education
ISO/IEC 17024 International Standard	Conformity assessment - General requirements for bodies operating certifications of persons	Security Defenders Certification
ISO 29993:2017 ⁵⁹	ISO 29993:2017 specifies requirements for learning services outside formal education, including vocational and in-company training.	Security Defender Education

Table 20: Education standards, regulations, and established recommendations of relevance for GEIGER

3.5 Selection of Standards and Regulations for GEIGER

As shown in the previous paragraph, many standards and regulations are potentially applicable to GEIGER. We here explore the potential applicability of these standards for the design, implementation, and management of the GEIGER solution and ecosystem.

3.5.1 GEIGER Solution

The GEIGER Solution comprises the technical framework, including the GEIGER indicator, toolbox, incident handling, information sharing and analysis with competent CERTs, and the security defender education and certification. It also includes the overall method which integrates the

⁵² <https://sec.eff.org/>

⁵³ <https://www.isaca.org/training-and-events/cybersecurity>

⁵⁴ <https://www.comptia.org/certifications?level=cybersecurity>

⁵⁵ <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html>

⁵⁶ <https://www.netacad.com/courses/cybersecurity>

⁵⁷ <https://www.globalcyberacademy.com/#courses>

⁵⁸ <https://cybersec4europe.eu/wp-content/uploads/2020/06/D6.1-Case-Pilot-for-WP2-Governance-V4-.pdf>

⁵⁹ <https://www.iso.org/standard/70357.html>

technical framework and Security Defenders education for reaching, motivating, and helping MSEs to become more secure.

For the **GEIGER Method**, the ISO/IEC 27'000 family of standards, the NIST cybersecurity framework, the AFM principles for information security can provide suitable guidance. They outline how information security risks can be managed with appropriate controls within an organisation. Also, the ISO/IEC 29100 family of standards and the NIST privacy framework can provide comparable guidance for managing privacy in an organisation. The maturity models developed by the University of Utrecht offer a complementary view of how to aggregate deployed tools and knowledge to increase the maturity of the SME.

The challenge for the application of these standards in GEIGER will be that they have been written with large organisations or critical infrastructures in mind. The necessary simplicity may be achieved by adopting a threat-oriented approach (as opposed to maturity), letting the MSE end-user work on one threat after the other, and spreading the organisation needed for managing cybersecurity across the GEIGER ecosystem.

For the **GEIGER Indicator**, The ISO 31000 family of standards, the NIST risk management framework, ETSI GS ISI 003, the ISACA Guide Cyber Security Check can provide comprehensive input for cybersecurity and data protection risk assessment and mitigation in an organisation. These standards offer a basis to ground the risk assessment performed by the GEIGER Indicator.

Assessments simplified for SMEs include the ICT Switzerland Cybersecurity Quick Check for SME and the Cybersecurity Raad Health Check. These quick checks offer visualisation and language that could make GEIGER accessible for MSEs. A more specialised assessment that assumes specific infrastructure is the NCCIC ICS Cyber Security Evaluation Tool.

The German BSI IT-Grundschutz Kompendium and the MITRE ATT&CK database offer knowledge relating threats with mechanisms for protecting an organisation and its assets. This knowledge can be useful for modelling and curating GEIGER recommendations offered to MSEs for protection against selected threats.

For **GEIGER Incident Handling**, the NIST Computer Security Incident Handling Guide can provide suitable guidance. It describes how capabilities for computer security incident response can be established and incidents handled efficiently and effectively.

The challenge for the application of this guide in GEIGER will be that it has been written with large organisations or critical infrastructures in mind. The necessary simplicity may be achieved by spreading the organisation needed for handling incidents across the GEIGER ecosystem.

For **GEIGER Information Sharing and Analysis**, MISP information exchange and data modelling can provide a basis for encoding information shared between GEIGER and CERTs. This information could include threat information and recommendations received from CERTs and MSE community profiles, and incident reports for analysis by CERTs. The ENISA Reference Incident Classification and the related MISP Taxonomies and Classification can offer a classification of incidents and corresponding threats enabling analysis of threats and reasoning about them. Information about knowledge of MSE employees could be encoded based on the Experience API.

The challenge to be addressed by GEIGER will be to adapt the content of the shared information to the entities that are meaningful for communicating risk to MSEs and protecting these MSEs. The MISP community data models can provide examples of how to create such domain-specific adaptations.

For **GEIGER Security Defenders**, the NIST NICE cybersecurity workforce framework and the Swiss ICT competence framework can provide a basis for the definition of profiles of professionals competent in cybersecurity. The challenge for GEIGER will be to curate the role profiles of level 1-4

Security Defenders in a way that education will be efficient and the resulting support for MSEs effective.

The NIST small business cybersecurity corner, the ACM cybersecurity education framework, and the EFF security education companion can provide content useful for education. The ISACA CSX cybersecurity nexus training and credentialing, the CompTIA cybersecurity certifications, the CISCO security certifications, and the global cyber academy courses offer examples of entry-level cybersecurity education with a matching certification. GEIGER will need to position its Security Defenders education within these frameworks and against these alternative training offerings. The specific security defenders profile will justify that positioning.

The quality assurance for CyberSec4Europe MOOCs can provide the first basis for quality assurance of the GEIGER Security Defenders education. The quality assurance approach will need to be adapted as GEIGER aims at integrating education in strategies other than MOOCs. Also, ISO 29993:2017 will be useful for quality assurance as it describes requirements for learning services, many of which are applicable also for GEIGER.

Finally, ISO/IEC 17024 describes how to allocate curriculum definition, education, and certifications to organisations. GEIGER will need to map this allocation to actors in the GEIGER ecosystem. SCORM 2004 will be useful to encode learning content to achieve interoperability with educators' learning management systems. The Experience API will be useful to achieve the same for tools and certifiers reporting learning outcomes of security defenders.

3.5.2 GEIGER Ecosystem

The GEIGER ecosystem consists of end-user SMEs, tool developers that provide tools for protection, education, and recommendation, CERTs for security information analysis and risk communication, and educators/certifiers with associated security experts for educating security defenders that can help MSEs.

The information sharing and analysis interfaces with the CERTs and curriculum/certification interface with educators/certifiers have been described above already. New here is the definition of MSEs and the positioning of the GEIGER project and future organisation. No clearly applicable standard, regulation, or recommendation could be identified for interoperability with tools provided by the GEIGER partner and third-party tool developers.

For **defining the GEIGER categories of MSEs**, the European Commission's SME and the European Digital SME Alliance's definition of SME types is useful. The former differentiates SMEs by size, the latter by the SME's position in the digital value chain. An observation important for GEIGER is that none of these taxonomies differentiates SMEs based on the need for help in improving their cybersecurity. This aspect fundamentally affects the GEIGER methodology.

Standards and policies applicable for any MSE include the General Data Protection Regulation (GDPR), the EDPB guidelines for controllers and processors of personal data, and the CNIL guides and templates for assisting data processors. For the coverage of Swiss law, the Swiss Federal Act on Data Protection will need to be used.

Several standards have been developed with digital enabler MSEs in mind: SMEs that produce ICT. These standards include the ENISA EUCC cybersecurity certification, the 3GPP and GSMA NESAS, and the CNIL guides and templates for developers.

For **positioning the GEIGER project**, the European Commission's skills for SMEs roadmap can be useful. GEIGER represents an instrument interesting for society, economy, and politics. As such, the roadmap can offer a basis for stimulating inputs for influencing policy based on observations made in the GEIGER project.

3.6 Expected Contributions to Standards and Policy

For GEIGER, the most attractive areas for contributions are the following ones: (C1) the Security Defenders education and certification, (C2) the interoperability with third-party tools for sensing, protecting, guiding, and educating cybersecurity and data protection of MSEs, (C3) the information sharing between GEIGER and CERTs, and (C4) policy definition for the protection of small businesses that depend on the use of social networks and public cloud providers. This section describes and motivates the expected contributions in each of these four areas.

3.6.1 C1: Security Defenders Curriculum

A large number of MSEs depend on help for protecting themselves against cyber threats and negligence in data protection. That large volume of help can only be provided if enough people are educated in the application of suitable tools in the MSE infrastructure and training of MSE employees. That large volume of training, again, can only be met with a matching number of training offerings provided by schools, associations, and other training organisations and with matching networks for offering certification examinations.

The case of the apprentices' school BBB shows the need for integrating such education as blocks in a larger educational curriculum for each specific profession. Hence, there is a need to position the GEIGER Security Defenders education within the professions' educational curricula and reach consensus regarding the size and scope of the Security Defenders education. BBB intends to facilitate the discussions necessary for obtaining the support of the Swiss ICT⁶⁰ and hairdressers⁶¹ professional associations. For further establishing the training, the support of other professional associations and schools like BBB is needed.

The case of SRA shows the scenario of a professional association developing and offering its own training to enable their associated professionals to offer specialised cybersecurity and data protection help as a service to MSEs. Here, support needs to be gained regarding the usefulness, feasibility, and business value of the education. These values, again, are based on the size and scope of the Security Defenders education. SRA intends to facilitate the discussions necessary for obtaining the support of the trainers and members. For further establishing the training, the support of the European umbrella organisation Accountancy Europe⁶² and its members in European member states other than the Netherlands need to be obtained.

The case of the innovation ecosystem of CLUJ IT resembles the case of SRA except that entrepreneurs, rather than accountants, will benefit from the education. CLUJ IT intends to facilitate the discussions necessary for obtaining the support of their trainers and members. For further establishing the training, the support of peer innovation ecosystems and, similarly, digital innovation hubs within Romania and across Europe need to be obtained.

The aim of the contribution C1 is to build momentum on the Security Defenders education efforts in the Swiss, Romanian, and Dutch use cases. Such momentum can be created by making the GEIGER efforts visible and engaging in discussion with the mentioned stakeholder organisations. The dialogue will aim at anchoring the relevant parts of the Security Defenders curriculum in the respective curricula and course offerings. The eventually obtained support and endorsement of these organisations will confirm the validity of the possibly adapted Security Defenders curriculum and establish trust in the Security Defenders education.

⁶⁰ <https://www.ict-berufsbildung.ch/>

⁶¹ <https://coiffuresuisse.ch/>

⁶² <https://www.accountancyeurope.eu/>

3.6.2 C2: Open Security Tools API

The cybersecurity market is vibrant and growing. The Forbes 2020 roundup of cybersecurity forecasts and market estimates report⁶³ indicates more than 10 billion € spending by 2023 – a figure that will have doubled in comparison to the corresponding expenditure in 2018. This spending stimulates a large number of tools being developed for sensing, recommending, protecting, and educating enterprises in cybersecurity. New tools continuously enter the market in reacting to the ever-changing threat landscape and new cybersecurity technologies that continue to emerge.

The consequence of the vibrant cybersecurity market is for GEIGER that no choice of tools for integration in the GEIGER Toolbox can be considered to be final. There are always new tools that should be considered, for example, because they are more efficient, more effective, or fit the specific needs and preferences of some MSEs better than others.

The contribution C2 aims at defining and establishing an open API allowing tools to be integrated into the GEIGER toolbox. The API is intended to create innovation potential by opening up the large community of MSEs as a market to tools providers and allow MSEs to benefit from attractive tools offerings. The GEIGER tool-developing partners will be substantial in the definition and validation of the API. Third-party tool developers willing to engage in the necessary dialogue with GEIGER can offer external validation of the API.

GEIGER will choose an approach influenced by successful app store ecosystems to define the interface. The definition will include the API specifications and associated data exchange protocols, user interface (UI) guidelines, and constraints for end-user license agreements (EULA). Compliance with three aspects will be used for any tool to be considered and recommended by the GEIGER framework. The design of the API, the UI guidelines, and the EULA constraints will be drafted first together with the tools partners in the GEIGER consortium and refined with third-party tool developers reached in collaboration with dissemination. Discussions with CEN/CLC/JTC 13 WG4, ISO/IEC JTC 27 WG4, and ECSO WG1 will be initiated to explore the proposition of the C2 open API for inclusion in their standardisation efforts.

Any contributions related to the interoperability with tools that report MSE employees learning outcomes will be based on the Experience API as much as possible. The classification of learning content recommended by integrated recommender tools will be based on the terminology and concepts proposed by ISO 29993:2017 and SCORM as applicable.

Interesting for GEIGER may also be to apply for the ECSO "Cybersecurity made in Europe"™ label⁶⁴. The label could support the exploitation of GEIGER in that it offers a differentiator based on the geographic location and the trust associated with cybersecurity from European organisations for the European market.

3.6.3 C3: Information Sharing and Analysis API

With the NIS Directive⁶⁵, the supervision of cybersecurity has become an important responsibility of each member state. In addition to supervising critical market operators such as energy, transport, health, and finance, member states are also turning to the supervision of the cybersecurity of SMEs. According to the Annual Report on European SMEs 2018/2019⁶⁶, SMEs represent more than 99% of the enterprises in Europe, produce more than 50% of the economic value, and offer about 2/3 of the

⁶³ <https://www.forbes.com/sites/louiscolombus/2020/04/05/2020-roundup-of-cybersecurity-forecasts-and-market-estimates/?sh=72de49b0381d>

⁶⁴ <https://www.ecs-org.eu/working-groups/cybersecurity-made-in-europe-label>

⁶⁵ <http://data.europa.eu/eli/dir/2016/1148/oj>

⁶⁶ <https://ec.europa.eu/docsroom/documents/38365/attachments/2/translations/en/renditions/native>

total employment. Hence, the SMEs, together as a whole, represent one of Europe's most critical sectors.

GEIGER aims at establishing a significant cybersecurity ecosystem for SMEs. Pursuing that aim, GEIGER will become an information sharing and analysis centre (ISAC). The GEIGER Framework will be the platform used for disseminating information about threats with associated recommendations in a personalised manner. The GEIGER Framework will also analyse information about the SMEs and the incidents they encounter. For a given MSE, threat information with associated recommendations is expected to originate mainly from the CERT that is competent for the MSE. To allow the CERT offer high-quality information and recommendations, the GEIGER framework will communicate relevant community information and incident reports from the consenting MSEs.

The aim of the contribution C3 is to define and establish an open ISAC API allowing CERTs to interoperate with GEIGER and vice-versa. The API is intended to create innovation potential by allowing any competent CERT to connect and interact with the MSEs for which the CERT is competent.

C3 will be addressed with an open Information Sharing and Analysis API that will be defined, implemented, and tried in collaboration with the GEIGER Romanian CERT CERT-RO and third-party CERTs collaborating with the GEIGER project, such as the Swiss NCSC. GEIGER will build on the open MISP standard⁶⁷ that is already established and in use for threat intelligence and information sharing.

In addition to the already involved CERTs, GEIGER will seek collaboration with even further CERTs and CSIRTs such as the Dutch Digital Trust Center and other organisations registered in the ENISA CSIRTs network⁶⁸. Also, GEIGER will establish liaison with initiatives like X-ISAC to seek synergies in the attempt of defining a stable and well-accepted ISAC API.

3.6.4 C4: Protection of MSEs whose Business depends on Social Networks and Cloud-based Services under non-European Ownership⁶⁹

Many MSEs depend on social networks for managing and running their business. Social networks are being used as a marketing channel informing customers about developments and news about the business as well as for offering paid services to subscribing customers. In both cases, social networks are used as a customer relationship management (CRM) system with customer contact information being stored. In the latter case, the social network is used to charge customers and track payment transaction. Both types of usage make the MSE vulnerable to a type of attack that has received little attention so far but has become critical for an increasing number of MSEs: an account blocking or deletion attack.

The case of the GEIGER use case MSE Coiffure Loredana illustrates the vulnerability for the account blocking attack well. Loredana uses Instagram and Facebook to inform customers about her business and any news associated with it. Loredana uses Pinterest to collect ideas about hairstyles and exchanging these ideas with customers. Finally, Loredana uses Whatsapp to manage customer contacts and discuss appointments with these customers. Hence, Coiffure Loredana manages data and runs its business in full dependency of these social networks. Her potential problem is that these social networks are owned by entities located outside the European jurisdiction: Facebook in Palo Alto, USA, and Pinterest in San Francisco, USA.

⁶⁷ <https://www.misp-project.org/>

⁶⁸ <https://www.enisa.europa.eu/topics/csirts-in-europe/csirts-network>

⁶⁹ With “Non-European” we anticipate the Brexit valid on December 31, 2020, where the UK will not be a EU member state anymore.

Similarly, Coiffure Loredana depends on the foreign cloud service SumUp to collect payments, manage payment transactions, and receive the resulting credit balance paid out for her company. SumUp is located in London, UK. Sum-up shares several characteristics with the before-mentioned social network: Loredana is expected to maintain an account and manage personal customer data in the form of payment transactions on the SumUp server. Additionally, Loredana manages some of her company's funds on the platform.

The following table summarises Coiffure Loredana's use of social networks and foreign cloud services.

Social Network / Foreign Cloud Service	Business Processes	Data
Instagram	Customer Relationship Management, Advertisement	Personal contact information, Advertisement campaign
Facebook	Customer Relationship Management, Advertisement	Personal contact information, Advertisement campaign
Pinterest	Consultancy Service	Knowledge base for hairstyles, incl. customer preferences
Whatsapp	Customer Relationship Management, Sales, and Support	Personal contact information and log of exchanged messages
Sum Up	Payment transactions and company's credit balance	Customer information used for performing payments and needed for taxation reporting

Table 21: Coiffure Loredana's use of social networks and foreign cloud services

The use of these social networks and foreign cloud-based services implies risks for Coiffure Loredana in relation to the blocking or deletion of her account and the consequent unavailability of data, infrastructure, and funds hurting Loredana's business.

For the account blocking or deletion attack to be successful, the service provider needs to believe an infringement of Loredana with the terms and conditions of using the service. For example, the Facebook Terms of Service state: "*We employ dedicated teams around the world and develop advanced technical systems to detect misuse of our Products, harmful conduct towards others, and situations where we may be able to help support or protect our community. If we learn of content or conduct like this, we will take appropriate action - for example, offering help, removing content, blocking access to certain features, disabling an account, or contacting law enforcement.*" The consequence of a suspected infringement is disabling an account without the possibility to retrieve the important business data and other assets associated with it.

Problematic for Loredana is that the service provider can decide to disable access for Loredana without any clear pre-notification or way to get in contact with the service provider. Also, if Loredana would like to resolve a dispute, she would be expected to approach a court outside the country in which her business is registered and active. Given Loredana's lack of experience and the small overall economic value of her assets, this requirement of calling a foreign court blocks any attempt for dispute resolution for Loredana.

Problematic for Loredana is also the lack of control over the mechanisms that could lead to Loredana's account being blocked. The automated algorithms the service providers use exposes Loredana to the limitations of the Artificial Intelligence that decides about account blocking. Also, she could be exposed to malicious actors who submit false reports to the service provider. A similar

outcome can be achieved by a change of her brand, e-mail address, or online domain name. Such a change can imply that Loredana loses access to her account without sufficient means to convince the service provider about her identity. A too easy way to change the account holder, however, could increase Loredana's risk of a malicious third party stealing her identity – again with the same consequences for Loredana of being blocked access to her account.

Problematic for Loredana, finally, is that no means are provided for her protection. For example, an effective approach to reducing the risk of losing access to data would be to do a backup of that data. However, none of these services would allow Loredana to do any such backup in a way effective for increasing her company's resilience.

The contribution C4 aims at working towards a regulation, respectively contributing to regulatory efforts that allow micro, small, and medium-sized enterprises to get protected against such account blocking attacks. The GEIGER project is in an excellent position to collect cases of MSEs exposed to the problem, or even having experienced such account blocking attacks. GEIGER is interested in exposing the problem, finding peers and stakeholders interested in addressing the problem, and engaging in the steps necessary to eventually bring about legislative change giving the MSEs the right to pursue mitigating actions and resolve disputes in an easy and cost-efficient way.

3.7 Summary and Conclusions

This section has given an overview of standards-defining organisations and initiatives that are related to the GEIGER project. Also, it listed standards, regulations, and guidelines useful for designing, implementing, and operating the GEIGER solution and ecosystem. Based on gaps observed during the requirements analysis of GEIGER, for areas have been identified where contributions to standardisation and policy definition from the GEIGER work can be expected.

The selection of standards and regulations will be used in the detailed definition of the GEIGER architecture (Task 1.2) and GEIGER indicator (Task 1.3). They will also be useful in guiding the implementation of the GEIGER framework (WP2) and security defender education (WP3). Task 5.2 will build on the work and lessons learned in the GEIGER project for producing the contributions in the areas C1-C4 based on a suitable dialogue with the identified stakeholders and in collaboration with dissemination (Task 5.1).

4 T5.3 Exploitation planning

4.1 Introduction

Building on the validation and demonstration results achieved in WP4 (Validation and Demonstration) and dissemination experiences in T5.1, a business model for the GEIGER organisation and an implementation strategy with recommendations for rolling out GEIGER across Europe will be developed. The business model will be based on market analysis and the lessons-learned from prototype demonstrations performed in operational environments, considering the value proposition for end-users (MSEs and “Security Defenders”), integrated tools and service providers (CSIRTs/CERTs and cyber ranges), and educational stakeholders as well as the resources needed to offer the GEIGER platform and education.

A financial analysis with multiple business development scenarios will be performed to identify a viable approach for implementing and rolling out GEIGER across Europe. The financial analysis will include revenue from end-users and partners within the GEIGER Ecosystem, ramp-up costs to establish and deploy GEIGER and costs to operate, maintain, and expand GEIGER. Based on the financial analysis, different funding scenarios will be identified and the creation of the GEIGER organisation prepared that will offer and maintain the GEIGER solution under the governance of the GEIGER ecosystem.

4.2 Approach and methodology

The GEIGER partners will prepare the jointly developed innovation, the GEIGER Solution, for sustainable rollout across Europe. A cornerstone will be the launch of an organisation, the GEIGER organisation, as a jointly created legal entity that will own and govern the associated intellectual property rights (IPR). The GEIGER organisation will provide the opportunity for open governance of the GEIGER Solution by firms such as established SME associations, educators, and CERTs that can offer needed market and industry knowledge, a factor critical for the success or failure of any platform.

To guarantee the continuation of the tools and ecosystem built during the project, the GEIGER project will initiate an organisation, a start-up company for managing and evolving the GEIGER Framework for joint exploitation. The organisation will be legally registered, own the necessary IPR for joint exploitation, and operate according to defined bylaws and business model for sustainability.

Create a novel SME as an exploitation entity. Governance by SME associations and other partners to bring in “sales knowledge towards SMEs.” IPR Handover and Ownership. The business management will need to be responsive to country-specific needs and policies of European Member states in relation to SMEs&MEs’ obligations to report incidents as well as to maintain synergy cybersecurity education and provision of tools and services for SMEs&MEs.

The business plan will assess the value proposition, pricing, required resources, and costs associated with the deployment of an EU-wide framework for risk analysis, communication, and reduction. It will explore different funding scenarios with a view to provide specific guidance to deploy a viable and sustainable service throughout the EU Member States. The sustainability of the approach will largely depend on an accurate assessment of the cost as well as the end-users' and stakeholders' willingness to pay for the assessment service, advice and tools for risk reduction, and education and examination services for the established Certified Security Defenders.

In particular, a key outcome of the project will be a detailed analysis of the pricing of the value proposition and costing of the resources needed during the initial phase. The analysis will be based

on pricing that is compatible with the low budget of MSEs for security and the large number of these companies, offering a viable alternative in comparison to services designed for large companies.

4.2.1 Pathway to impact through exploitation planning

Exploitation is about innovation. A successful exploitation plan strongly depends on the innovation plan. This requires application of a proper innovation model. The innovation model has three dimensions: product (solution), market, and company (start-up). Each of the three layers has its life cycle. To succeed we need the proper timing of the three life cycles.

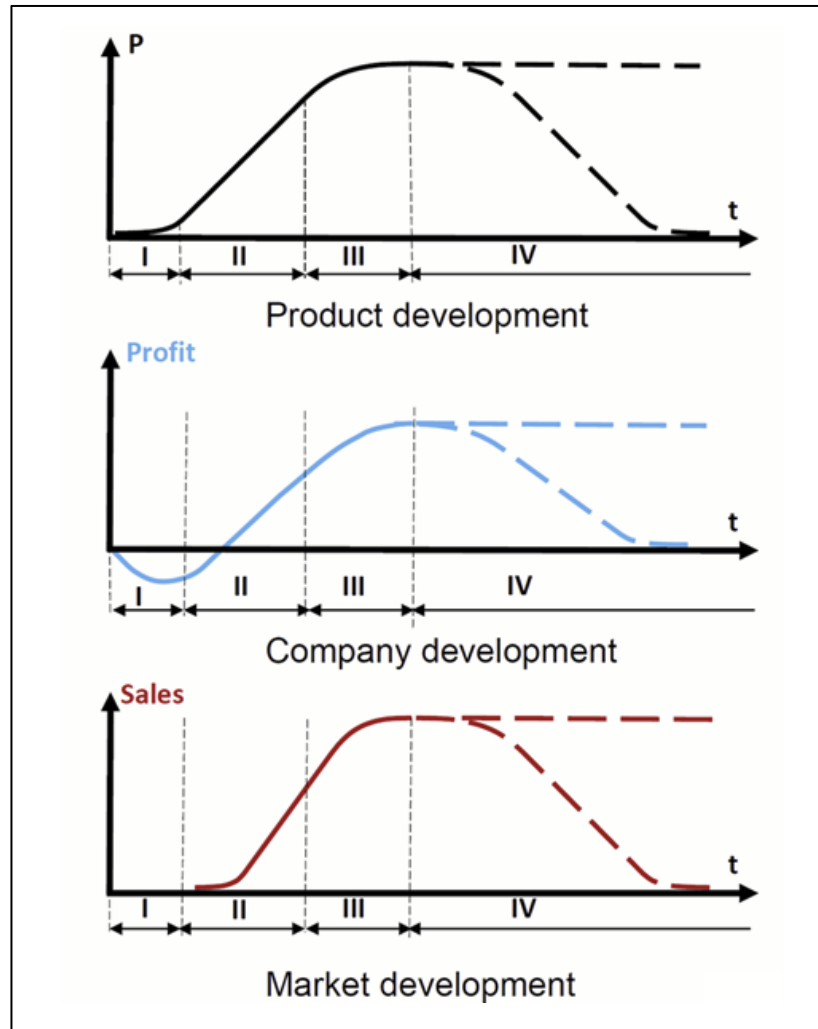


Figure 22: The three life cycles

In the particular case of GEIGER, we have the following situation:

- market (MSEs) needs more education and awareness to adopt the GEIGER solution package;
- technology starts from the TRL1 stage, with possible infusion of solutions from TRL6 in some areas;
- technology must reach TRL6 or TRL7 at the end of the project in order to position the GEIGER business in the stage where venture capital can be attracted; and
- company (the start-up) must be prepared early to get the critical mass of inputs at the end of the project.

There are several combinations of the three life cycles, as it is shown below:

Development Objects	Stages of development			
Product	P1	P2	P3	P4
Company	C1	C2	C3	C4
Market	M1	M2	M3	M4

Figure 23: Combinations of the three life cycles

A list of 64 combinations of stages of the three life cycles can exist, some of them being highlighted below:

- **The best** – P1C1M2, P1C2M1, P2C2M2, P3C3M3, P3C3M4, P4C3M4.
- **Real** – P2C1M1, P2C2M1, P3C2M3, P3C2M2, P3C2M1.
- **Unreal (undesirable)** – P3C1M3, P3C1M2, P1C2M3.

Figure 24: Possible combinations of the life cycle stages

GEIGER must adopt a strategy for disruptive innovation to succeed in the highly competitive market of cybersecurity solutions. In this respect, GEIGER must focus on a strategy from category **“best”**. From the pool of strategies, the selected variant (option) is: **P2C2M2**. This means:

- product reaches TRL6 or TRL7
- company advances to the level of being ready to attract venture capital immediately after the end of the GEIGER project
- a critical number of MSEs are educated and ready to adopt GEIGER solution immediately

To meet this position, we need to adopt the **lean start-up** innovation model. This requires a specific approach within the GEIGER project, as indicated in the table below.

Stage	Methods	Who	Tests	Who	Check results
Ideation	Focus groups Contextual analysis JTBD Empathy Systematic ideation	WP1	Voting Proof tests	All partners Potential beneficiaries	Value for users Novelties Key features
Problem	Ethnography Pains and cause-effect	WP1	Cold call test Smoke test	Potential beneficiaries	Market segments Personas Vision Value proposition [1 st iteration]
Solution	Brainstorming 6H Near-Far Parts-Whole Visible-Invisible Pugh selection	WP2, WP3	WOW test Promoter test Right price (value) test 9x test	Potential beneficiaries	Theoretical prototype (several instances) Mock-ups Demos on key features MVP Beta Version 1.0
Go-to-market	Value proposition design Price strategy Sales strategy Delivery strategy Key activities Key resources Pivoting strategies of business model	WP5	Innovations on business model	Potential beneficiaries	Business model [1 st version] Business model [variants] Final business model
Scaling-up	Assessments	WP5	Innovations on business processes and value chains	Potential beneficiaries investors	Team Processes Markets

Table 22: Lean start-up flow

According to data in the above table, we must start the exploitation plan interdependent and simultaneously with the development of the product (Solution). Thus, we need to **impose** the role of **Product Manager** in the project with authority to negotiate with the development team and to monitor the maturity and quality of the product during its life cycle stages. Monitoring and negotiation must be based on FACTS collected from the potential market (beneficiaries). This involves the application of various tests in different stages of product development.

Additionally, the lean innovation process must be correlated with the TRL evolution of the GEIGER solution. This is illustrated in the following figure.

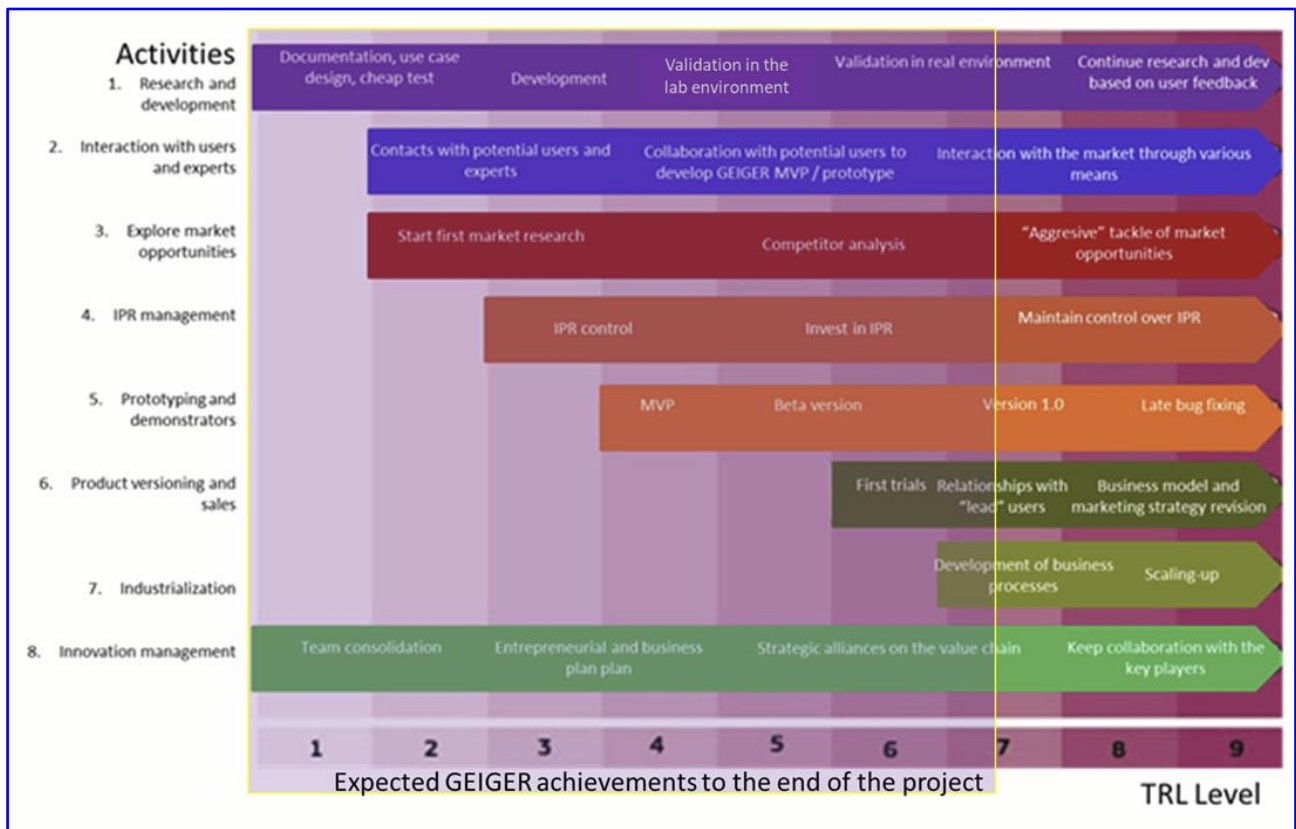


Figure 25: Technology Readiness Level (TRL) and correlation with the GEIGER innovation process

From a product innovation strategy point of view, the need for disruptive product innovation is a **must**. This is also imposed by the category of major beneficiaries: MEs and SMEs, which necessitates both an affordable business model and prices, and a focus on those organizational functions and goals that are more pregnant in the case of MEs and SMEs (e.g. cyber-attacks related to financial aspects than data breach aspects). The graphical representation of this strategy is shown below.

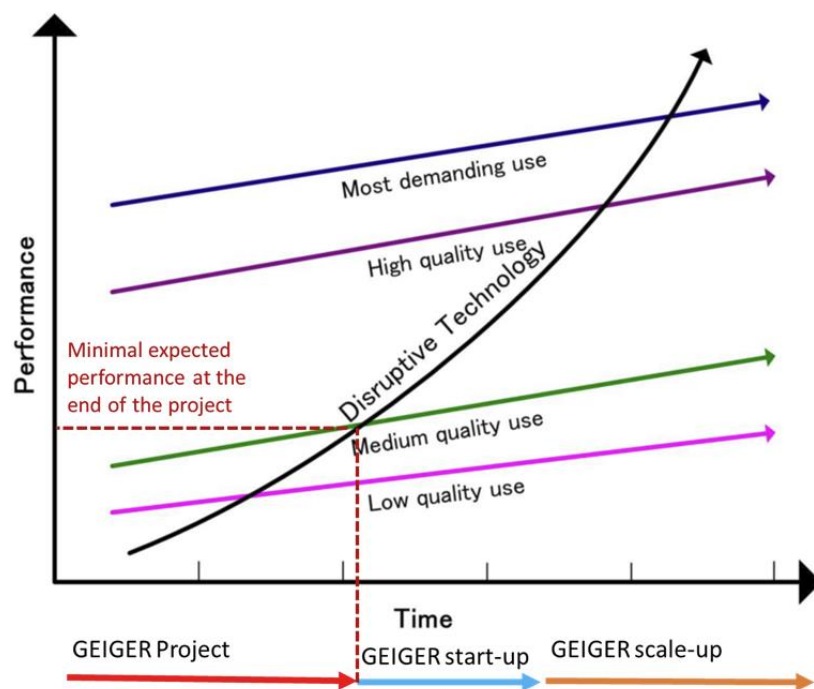


Figure 26: Disruptive innovation strategy for the GEIGER solution

To operationalise the disruptive innovation strategy, we need to adopt a specialised strategy at product level. This specialised strategy, based on the laws of directed system evolution and disruption paradigm should look like in the figure below:

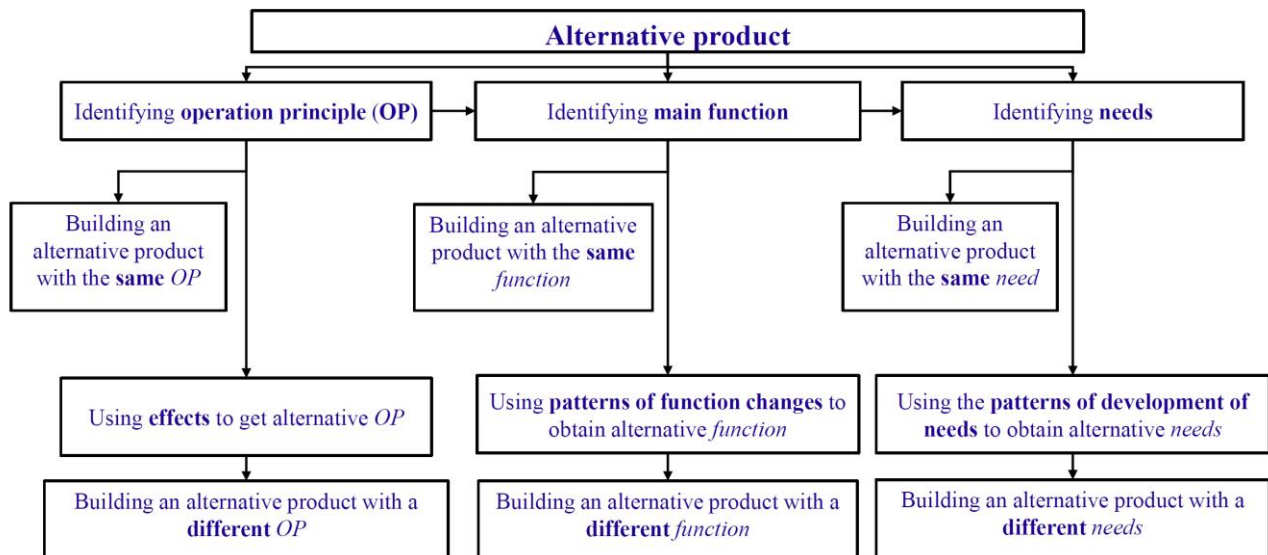


Figure 27: GEIGER must be directed for the creation of a fundamentally new product

In relation to product strategy, an interaction of the development team with the team responsible for requirements engineering (using close interaction with the end users) is taken into account such as the AGILE process for cyber-GEIGER development to be done in a robust way in terms of fast adoption by the market. Co-creation using various methods and tests is considered in the methodology. Thus, the phase called “Problem” in the Lean Innovation Methodology is crucial to define the vision and value proposition.

To bring the market’s life cycle in phase 2, to be in conformance with the P2C2M2 option for launching the cyber-GEIGER onto the market, the strategy must involve:

- having a dense process of education (evangelism) at MEs&SMEs level in as many as markets as possible during the duration of the GEIGER project (the target should be of at least 500 companies becoming aware and motivated to adopt cyber-GEIGER immediately)
- running the training of cyber-defenders on a critical mass of persons from different target markets (100+)
- to introduce the cyber-GEIGER to venture capitalists as soon as we have the first demos
- to run intensive information of the potential market (10000+ reaches)
- to have prepared the web interface with the market for easy communication (portal) during the period of the project
- to have several success stories and lead users in order to valorise this for promotion / advertising
- to test during the project in a critical mass of MEs&SMEs cyber-incidents (e.g. using CERTs support and specialised sensors) such as to have motivational content for being used in the interaction with the target markets

In terms of company/s maturity (the cyber-GEIGER start-up, in order to reach phase 2, we need to prepare the partnership starting with M18. This requires a clear understanding and completion of:

- the partners,
- the headquarter,
- the equity distribution,
- the model “equity-dividend”,
- the background IP framework,
- the IP valuation solution,
- the value chain generation partnership canvas,
- the capability-driven partner typecasting,
- the partnership (joint venture) agreement outline and steps.

In addition to these elements, at the end of the project we have to cover all elements highlighted in the Exploitation Plan, in the Lean Start-up Model and in the INSPIRE framework.

<p>Impact goal (change that will occur) Impact on SMEs Relation with the description of action (DoA) in the project proposal</p>	<ul style="list-style-type: none"> • More and more MEs and SMEs will dramatically change their attitude and interest in relation with the internal practices and capabilities on cybersecurity • On short term, a significant number of MEs and SMEs will adopt cyber-GEIGER SOLUTION (product-service system) • On mid-term, cybersecurity should be a familiar issue in the majority of MEs and SMEs, which allocate resources for education in cyber-sec, implement technologies and adapt their processes to reduce the risks on cyber-attacks
<p>Contribution towards European policy objectives and strategies Impact on policy making</p>	<ul style="list-style-type: none"> • The results of the GEIGER project will be aligned with the ENISA goals • The results are aligned with the strategic agenda of EC on cybersecurity and EC initiatives (ISACs, CSIRTs/CERTs, ESCO)
<p>Target stakeholders or publics Who will benefit?</p>	<ul style="list-style-type: none"> • MEs & SMEs • Employees from MEs & SMEs (better educated on cyber-sec issues, with huge impact on their extra-job interactions with the Internet - e-banking, e-shopping, etc.)
<p>Reasons for being interested in the GEIGER results</p>	<ul style="list-style-type: none"> • Calibrated to the needs of SMEs/MEs • Designed for users with non-IT background • Comprehensive ecosystem for cybersecurity support
<p>Pathway to impact Steps/activities that need to happen (and by whom) Activities to engage this target group</p>	<ul style="list-style-type: none"> • Lean Innovation • Agile/Co-creation • Deep interactions with end-users • Follow-up - start-up to continue cyber-GEIGER • Build up a partnership with EC Agencies (JRC, EASME, EEN) to promote cyber-GEIGER
<p>Evidence What will success look like and how can it be demonstrated? Indicators of successful engagement and means of measurement</p>	<ul style="list-style-type: none"> • The start-up will become functional and will succeed to raise funds for scaling-up
<p>Indicators of progress towards impact Means of measurement</p>	<ul style="list-style-type: none"> • The progressive market tests run during project running • The maturity of partnership to setup the start-up
<p>Risks and barriers to activities and mitigation</p>	<ul style="list-style-type: none"> • Budget allocated in the project too low relative to the expected conclusions generated in the requirements engineering phase [preventive action: quantitative planning 80-20 rule] • Lack of correlation between WP2, WP3, and WP4 with WP5 [preventive action: lean innovation model; 2-weeks inter-WP sessions for progress monitoring]

Risks and barriers to impact, and mitigation	<ul style="list-style-type: none"> • Level of commitment of the partners to become part/support the start-up launching [preventive action: early planning] • Insufficient planning of the entry strategy [preventive action: lean start-up process]
Responsible actors and resources	<ul style="list-style-type: none"> • Every partner has a certain level of impact on the final success • Need for early allocation of responsibilities on different chapters of the exploitation plan
Timing	<ul style="list-style-type: none"> • According to the Gantt chart

Table 23: Elements of the exploitation plan

4.2.2 Criteria for measuring success

Criteria to measure the impact success must cover all phases of the project lifecycle. This means, we have criteria that measure success from the perspective of preconditions (results) and criteria that are associated with outcomes. Exploitation must include multiple layers:

1. Financial exploitation, building product-service systems (cyber-GEIGER solution), new international projects, based on the project results;
2. R&D and innovation, by engaging new projects (Horizon Europe), based on the experiences gained in the GEIGER project;
3. Education and training at the university level and in the cyber-GEIGER network on the 4-layer model;
4. Community-building around the topic of cybersecurity, raising awareness and the propose solutions for SMEs and MEs;
5. Knowledge transfer, from academia to industry, by collaboration or scientific publications; and
6. Contributions to standardization.

Precondition-related metrics (ex-ante)

- Number of cybersecurity defenders enrolled in the in the GEIGER educational program
- Feedbacks about cyber-GEIGER solution from potential users & lead users in various prototyping phases
- Feedbacks of the trainees on the training materials
- Number of published papers in highly visible journals and conferences
- Number of published articles in magazines
- Number of visitors of the GEIGER website
- Number of MSEs/MEs reached and informed about the GEIGER presence
- Number of venture capitalists that asked details about cyber-GEIGER business

Postcondition-related metrics (ex-post)

- Number of universities that adopt courses on cybersecurity based on GEIGER educational materials
- Number of high school students enrolled in the GEIGER educational program
- Number of university students enrolled in the GEIGER educational program
- Number of cybersecurity defenders in 3 years and their territorial distribution
- Number of SMEs & MEs that adopted cyber-GEIGER in 3 years and their territorial distribution
- Contribution to cybersecurity standards at national level
- Contribution to cybersecurity standards at EU / European and international level

- New project in Horizon Europe as a follow up of GEIGER (e.g. infusion of AI and blockchain in the cyber-GEIGER solution)
- Functional start-up (cyber-GEIGER) and the level of capitalization & turnover in 3 years
- Satisfaction of adopters
- Satisfaction of trainees
- Number of citations of the papers published in scientific journals and conferences

4.3 Achievements to date

In the period M1-M6, for T5.3 we can report the following achievements:

- We created the detailed structure and template for the exploitation plan.
- We started applying the lean start-up methodology; to this date we tackled the “Ideation” phase with the application of all methods and tests.
- We discussed in the consortium how to approach the “Problem” phase and we are in preparation of meetings to cover the associated methodology and tests.
- We investigated how we can properly frame “open innovation” in the consortium in order to manage IP life cycle and quantify it in a secured mode.

With respect to the “open innovation” issue, we have investigated two frameworks. The first one is the INSPIRE platform dedicated to assist SMEs for open innovation. The second one is the DEIP platform, which is a hybrid blockchain-driven platform to protect and assess all IP contributions of the partners in the consortium and to link this results with a crowdfunding platform for speeding up the capitalization of the start-up at the end of the project. Our conclusion is that both frameworks should be integrated in the GEIGER’s practice to maximize the impact.

4.3.1 INSPIRE

INSPIRE (INtegrated Support of oPen Innovation pROfessionalization) initiative studied 120 SMEs from all over EU, between 2016 and 2019. The INSPIRE online platform as developed by the project can be seen and used online at <https://inspire-smes.eu/>. The INSPIRE online platform includes a series of inspirational case studies of successful Open Innovation projects in European SMEs, as well as many management tools which can be used to increase the chances of the Open Innovation project adding real and lasting value to the SME. The INSPIRE project was funded under the H2020 programme by the European Union in order to help and support SMEs in retaining more of the business value when engaging with Open Innovation activities. INSPIRE is set to understand and support the management of Open Innovation in SMEs. To fulfil this knowledge and practice gap, INSPIRE studies a critical mass of SME Open Innovation good practice cases and translates the findings into an Integrated Toolbox, a portal with resources appropriate for SMEs, their support agencies and other innovation practitioners in Europe.

Inspire Open Innovation – Methodology consists of:

- 114 cases (inspirational cases studies)
- 128 management tools



Figure 28: INSPIRE Canvas

INSPIRE CANVAS – guides SMEs throughout the entire OI process and helps to track progress.

INSPIRE has a challenge-oriented approach, in which the Innovation wheel has 3 phases **Exploration, Development, Commercialisation** (see Figure 28).

Exploration: For those companies wanting help with exploring opportunities or developing their concept. These are companies typically at the beginning of the innovation cycle.

Development: For those companies who have moved past the initial idea and set-up phase and need help validating their concept or introducing the product/service to market. These are companies typically in the middle of the innovation cycle.

Commercialisation: For those companies who have established their product/service and now need help with scaling-up or with expanding /diversifying their business. These are companies typically in the later stages of the innovation cycle.

SMEs can choose a challenge and the following are proposed by the platform: Cooperation Tools, General innovation tools, Support Resources, and Case Studies. The tools proposed by INSPIRE platform are classified as:

- Discussion tools
- Checklists
- Thinking Frameworks

4.3.1.1 Innovation Readiness Assessment

The Innovation Readiness Assessment tool allows a SME to understand how ready their business is to engage in strategic collaborative activities with individuals and other organisations in order to

innovate. The result will provide the readiness level, the current competitive position for each of the six stages of the innovation challenges (see Inspire Canvas), including recommendations.

4.3.1.2 The INSPIRE online challenges

There are six different pathways of the CHALLENGES part of the INSPIRE online platform, to guide SMEs to relevant resources and tools.

Phase	Stage	Description
Exploration	Explore Opportunity	<ul style="list-style-type: none"> - How to explore a new business idea - How to commercialize a technology/research results/IP - How to understand the possible applications of my innovation - How to understand if there is a market for my business idea - How to establish a new business model/business line
	Define Concept	<ul style="list-style-type: none"> - How to select the right application for my innovation - How to identify the competences I'm missing for designing/developing a new product/service - How to interact with potential customers to understand their needs in depth - How to co-create with potential customers
Development	Validate Concept	<ul style="list-style-type: none"> - How to make my product compliant with regulations/standards - How to test a new product/service - How to try out my new product/service with potential customers - How to understand the market my product/service targets How to create awareness for my product/service
	Introduce to Market	<ul style="list-style-type: none"> - How to introduce alone (internal exploitation) - How to introduce via partners (external exploitation) - How to do a joint exploitation (shared exploitation)
Commercialisation	Scale-Up	<ul style="list-style-type: none"> - How to spin off, spin out, create/join a new venture - How to find investors - How to scale up my organization (production, sales, after-sales)
	Expand & Diversify	<ul style="list-style-type: none"> - How to reach a new market - How to expand to international markets

Figure 29: The six pathways of the CHALLENGES part of the INSPIRE online platform

Once the strategic challenge(s) and objective(s) have been established, and the company has used some of the INSPIRE Toolbox resources if needed, the next step is to reflect on competence and resource gaps (i.e. the skills and knowledge the company is missing). This will help assess the possibilities for an open innovation partnership to help them reach their goal.

The corresponding tools and use cases are proposed by selecting a challenge, or by directly selecting an area thru Manage section of the INSPIRE Platform. The Manage section contains resources to support the partnership analysis and management of open innovation. As in the case of the challenges section, by selecting one of the areas of interest, a selection of different innovation management options are presented to explore, and by selecting a statement, a page with a series of proposed tools, cases studies and resources is opened.

4.3.1.3 Inventory of the tools proposed by INSPIRE platform

On the platform, there are (free and downloadable) 128 management tools with instructions to allow companies to determine their OI requirements and assess and determine their possible strategies. Some are proprietary and some are open-source or well known; but being in the one location and presented in convenient categories, the website makes access to these tools extremely convenient. Easy to use web-based platform. The system has been set up to make it easy for anyone to use. The case studies and relevant OI Management Tools are easy to access through an intuitive menu. Specifically, INSPIRE is a complete OI methodology that can be applied by any company, of any size, to any growth opportunity or requirement. It is easy to use and comprehensive in its coverage, helpful for SMEs at all different stages of development and in a whole range of sectors and situations.

For the Exploitation Plan, the following tools might be useful:

Introduce to market – Development phase		
Alone (internal exploitation)	Via partners (external exploitation)	Joint exploitation (shared exploitation) - the scenario of having the GEIGER start-up
<ol style="list-style-type: none"> 1. Make-or-Buy Decision Guide 2. Partner ecosystem mapping 3. Building a shared marketing resource plan 4. Cambridge technology compatibility tool 5. Cambridge technology absorption tool 6. Stakeholder analysis matrix 7. Building a marketing partnership map 8. Marketing strategy guiding framework 9. Social media marketing campaign canvas 10. Lean Canvas 11. Business Model Canvas 12. Marketing tactics 13. Marketing campaign template 	<ol style="list-style-type: none"> 1. Value chain generation partnership canvas 2. Make-or-Buy Decision Guide 3. Building a shared marketing resource plan 4. Capability-driven partner typecasting 5. Background IP framework 6. Partnership agreement outline and steps 7. Marketing Strategy guiding framework 8. IP Valuation 9. Lean Canvas 10. Business Model Canvas 11. Marketing tactics 12. Marketing campaign template 	<ol style="list-style-type: none"> 1. Partnership agreement outline and steps 2. Background IP framework 3. Capability-driven partner typecasting 4. Building a shared marketing resource plan 5. Value chain generation partnership canvas 6. Marketing tactics 7. Marketing campaign template 8. Lean Canvas 9. Business Model Canvas 10. IP Valuation 11. Marketing strategy guiding framework
Scale Up – Commercialisation		
How to spin off, spin out, create/join a new venture	How to find investors	How to scale up organisation (production, sales, aftersales)
<ol style="list-style-type: none"> 1. Lafley and Martin's Five-Step Strategy Model 2. Visioning Tools of OI Ventures 3. Pivot or proceed? 4. Marketing strategy guiding framework 5. Production Strategy Matrix 	<ol style="list-style-type: none"> 1. Value chain generation partnership canvas 2. Capability-driven partner typecasting 3. Redkite Partnership canvas 4. Minimum Viable Product Tools 5. IP Valuation 6. Sales message cheat sheet 	<ol style="list-style-type: none"> 1. Outsourcing Matrix 2. Make-or-Buy Decision Guide 3. Production Strategy Matrix 4. Pivot or proceed?

<ul style="list-style-type: none"> 6. IP checklist (patent and trademark) 7. 4 step Market opportunity evaluation tool 8. IP Valuation 9. Social media marketing campaign canvas 	<ul style="list-style-type: none"> 7. IP Checklist (patent & trademark) 	
Expand and Diversify – Commercialisation		
How to reach a new market	How to expand into international markets	
<ul style="list-style-type: none"> 1. Joint marketing plan 2. Building a shared marketing resource plan 3. Building a marketing partnership map 4. Marketing tactics 5. Marketing campaign checklist & planner 6. (Lead) customer persona 7. Social media marketing campaign canvas 8. Pivot or proceed? 9. Customer discovery (B2B, B2C) 10. Marketing strategy guiding framework 11. Marketing campaign template 	<ul style="list-style-type: none"> 1. Redkite Partnership canvas 2. Building a shared marketing resource plan 3. Cambridge motives for acquisition tool 4. Joint marketing plan 5. Social media marketing campaign canvas 6. Pivot or proceed? 7. Marketing strategy guiding framework 	

Table 24: Potentially useful tools for the GEIGER exploitation plan

The DEIP platform is a platform where the GEIGER project can collect all innovations done by all partners and instantly protects (as proof of ownership) the results using blockchain technology. In the platform one can create public and private spaces. All inputs are assessed on various weighted criteria. Input innovations can be of any kind, from marketing to technical or business model related, as well as market creation, or knowledge, or patents.

The platform also can be connected any time, at any moment of the TRL of the solution to a platform for fundraising. This is a very important feature to facilitate the capitalization of the start-up at the end of the GEIGER project. In this respect, we have started to prepare the framework for adopting the DEIP platform in the GEIGER project in relation to the Exploitation Plan. By adopting this solution for open research and innovation, as well as by connecting to a fundraising platform we can have an early perspective on the interest for various innovations embedded in the GEIGER solution and we can pivot during the development phase if this would be necessary. Figure below illustrates the DEIP platform entry- menu.

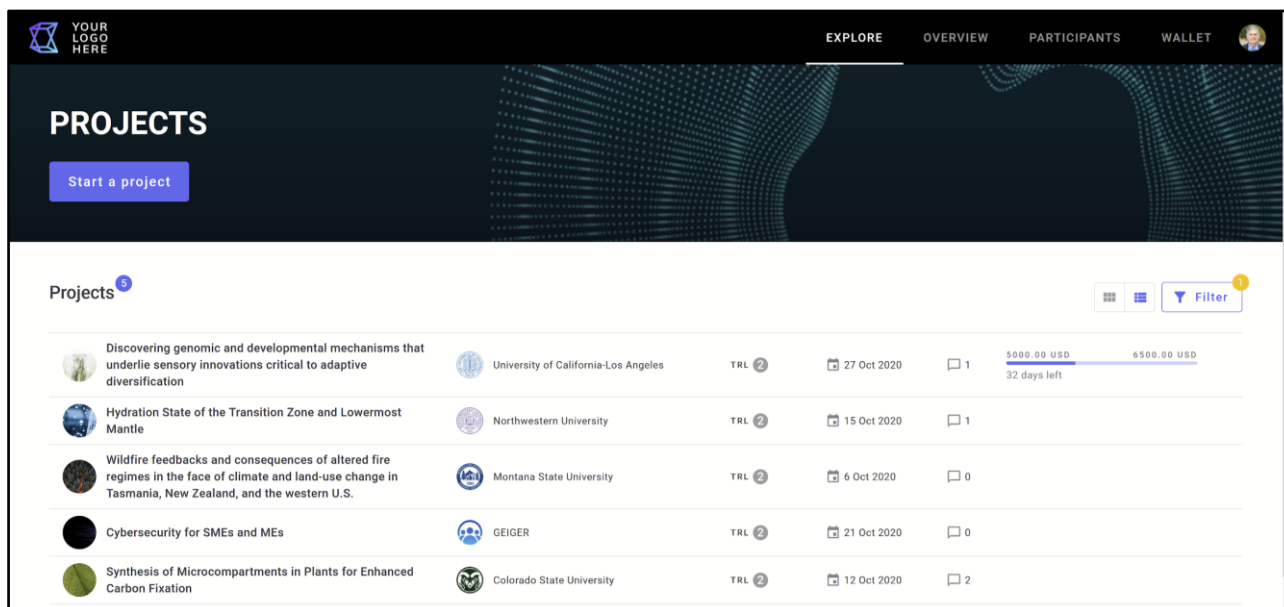


Figure 30: DEIP Platform

4.4 Impact Tracking

Tracking of the exploitation plan is related to any exploitable results of the GEIGER project with impact on the transformation of current practices in SMEs & MEs relative to cybersecurity issues. This means a strong connection between the project and the adopters of the cyber-GEIGER solution, as well as between the project and the entities involved in the exploitation of results to enhance their capabilities and value added of their services; the start-up, universities, CERTs/CSIRTs, consulting companies, cybersecurity solution developers (e.g. by licensing IPs from GEIGER), experts and cybersecurity defenders.

Impact tracking on adopters (SMEs, MEs, people):

- adoption of cyber-GEIGER shall be run through a commercial initiative (i.e. a start-up); thus, impact shall be countered by number of users that installed the system on their devices
- cybersecurity defenders and services provided in the market shall be countered through a web portal designed to manage these issues
- cyber-GEIGER educational program will be tracked by counting the users signed in the web portal and those who fulfil the program to receive the certificate

Impact tracking on entities that can use cyber-GEIGER to expand the value-added of their services:

- cyber-GEIGER will be accessible to third parties through the portal and based on a commercial partnership; the end beneficiaries will be counted through the portal and agreements with the third parties to register end beneficiaries in the portal

4.5 Summary and Conclusions

This section described our approach to the exploitation planning of the GEIGER project, and our initial vision of the business model for the GEIGER organisation and the strategy for rolling out GEIGER across Europe. It also listed the achievement under T5.3 during M1-M6 of the project.

Cyber-GEIGER should be a disruptive product-service system in the field of cybersecurity, calibrated to best fit the culture and needs of MSEs. It should cover the life cycle of a MSE journey to become highly secured in front of various cyber threats. Results will be valorised in the market by

means of a business initiative. Product-service/technology development, market education and business initiative should be well correlated to succeed. This requires a lean innovation approach, which must start from the very early stage of the project. Agile-lean development must be taken into account such as to achieve this goal. End-users must be continuously involved in the development process for probing-feedback-refining the solution. IP (background and foreground) must be properly managed and quantified to maximise the contribution of all partners in the projects. There are tools to be used in this respect.

To be successful and produce disruption, product innovation must follow a clear strategy (fundamentally different product) based on 6 rules. For adoption, the market should be evangelised to understand the necessity and to know how to approach the problem without big efforts. This involves a good coverage of the lead users group with smart designed education and training programs. The start-up must reach a critical point on its life cycle such as the transfer of the project's results to be done in a proper and timely manner. This necessitates the application of a list of methods to make things progress in a structured way.

5 Conclusion

In this Impact Plan, we presented an overview of GEIGER's objectives concerning the project's dissemination and communication plans, expected contributions to standardisation and policy definition, as well as our aspirations regarding the long-lasting impact beyond the duration of the project that we aim at achieving by the sustainable exploitation of the project results and the rollout of GEIGER across Europe.

This deliverable D5.1 will serve as the basis of the work of WP5, guiding the actions taken within the T5.1, T5.2 and T5.3. The visual design and presented mapping of standards will support the technical development in WP2 as well as the building of the education programme and ecosystem in WP3. The planned targeting of stakeholders will support the community-building in WP3 and the piloting of GEIGER Solution in WP4.

D5.1 is the first deliverable for the dissemination, standardisation, and exploitation planning activities of the GEIGER project. The plan will evolve throughout the project's lifespan and will be updated and adjusted on a regular basis with any new relevant outcomes that may impact our dissemination and communication, standardisation, and exploitation planning strategies. Any significant changes to the plan and the outcomes achieved by executing it will be documented in the future WP5 deliverables.