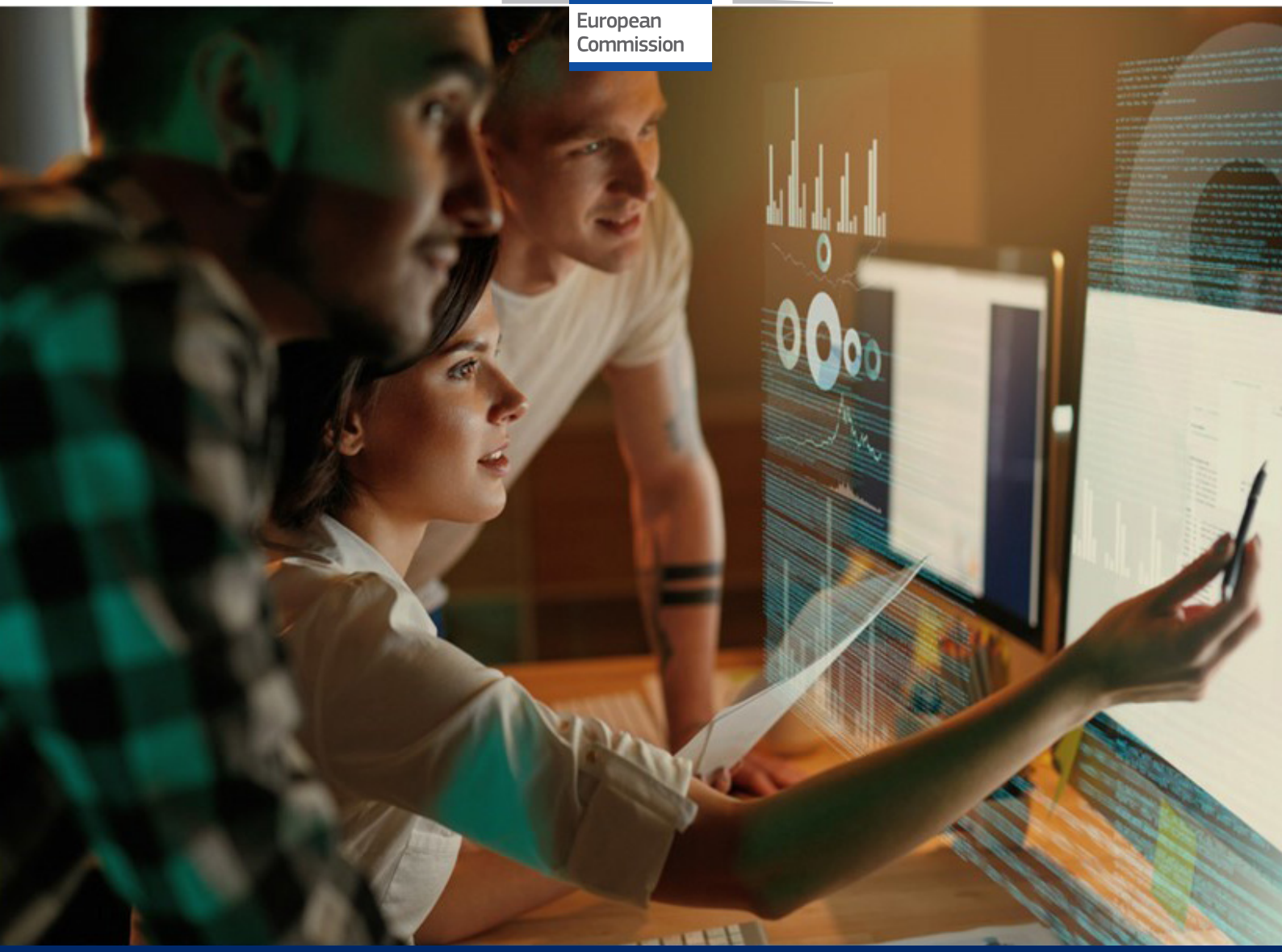
European Commission



Skills for SMEs

Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises

December 2019

Service Contract: Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity in SMEs
EASME/COSME/2017/007

For more information about this paper, please contact:

European Commission

European Commission
Executive Agency for Small and Medium-sized Enterprises (EASME)
Unit A.1.3 Entrepreneurship and Clusters

E-mail: EASME-COSME-ENQUIRIES@ec.europa.eu

European Commission
B-1049 Brussels

Acknowledgements
Our work would not have been possible without the generous participation of many experts. We are very grateful to the more than 200 professionals and stakeholders who took the time to share their views with us through interviews, workshops and other meetings.

ISBN: 978-92-9202-779-7
doi: 10.2826/708138

Skills for SMEs

Cybersecurity, Internet of Things and Big Data for Small and Medium-Sized Enterprises

Contents

Introduction

Digitisation of SMEs is an important and great challenge: from various evidence it is clear that SMEs are hesitant when it comes to adopting new technologies. Despite market volume or business growth opportunities, most SMEs keep lagging behind. And that is NOT going to help them on the long term. Cyber-risks are threatening business continuity. Companies using large amounts of data and the Internet of Things will manage to produce higher quality services or products at lower costs and push non-digital SMEs out of the market. European SMEs run the risk to miss out on the huge market potential. They are lacking the necessary skills and access to highly skilled graduates and experienced workers: there a fierce and increasing competition for talent. Research shows that already more than 90% of European SMEs consider themselves lagging behind in digital innovation.

The European Commission - Directorate-General Internal Market, Industry, Entrepreneurship and SMEs - launched an initiative on “Skills for SMEs” to analyse the root-causes and remedy to this situation. One element stands out: SMEs are increasingly under pressure as they compete with large companies on a tense job market. Significant skills related issues exist across company roles: there is a lack of digital leadership skills at the top, a shortage of IT professionals and severe lack of adequate skills amongst users. Skills shortages, gaps and mismatches hinder organisations to define their growth strategy, to implement it, and to enable employees to actually use new technologies.

Ambitious skills policies and well-targeted supporting measures at EU and national levels are thus needed to facilitate the access of SMEs to a larger European talent pool. Contracted by the European Commission to support the “Skills for SMEs” initiative, Capgemini Invent together with the DIGITAL SME Alliance and Technopolis researched, identified, designed, tested and validated such specific measures for supporting specialised skills development related to big data, Internet of Things and cybersecurity for SMEs in Europe.

This brochure is presenting a summary of the final report. It is proposing a shared vision, a roadmap and a toolbox that were created in close collaboration with hundreds of experts, SMEs and key stakeholders across Europe. The brochure “Skills for SMEs” complements several other publications under the Skills for Industry series.

A comprehensive strategy to support skills development in SMEs

Rationale for an SME-centred skills development strategy

The digital revolution is not only about large tech companies but also essentially about start-ups and small and medium-sized enterprises (SMEs) that provide or use digital solutions. **SMEs are vital to the European economy**, making up 99% of Europe's businesses and accounting for two-thirds of total employment. Their variety is huge, from innovative and fast-growing companies that provide or use digital solutions, to those that face significant challenges such as acquiring the necessary skills to benefit from digital technologies.

"While we are still coping now, the digital skills gap will hit us like a thunderstorm in the next years. We need a serious strategy to upskill the European workforce to keep our SMEs competitive."

Bo Sejer Frandsen, CEO it-forum, Vice-President of European DIGITAL SME Alliance, Board Member AIOTI

Given that improving basic digital skills is already a challenge, the emergence of technologies such as big data, internet of things (IoT) and cybersecurity is creating significant new specialised-skills gaps, shortages and mismatches, especially for SMEs, who cannot afford to compete with large enterprises to attract and retain the scarce digital talents. There are **serious skills shortages at every level in the hierarchy of SMEs**: from e-Leadership skills to ICT-professionals to users' digital skills. This is an issue, as European SMEs run the risk of missing out on a huge market potential. The German association Bitkom estimates the economic damage to German companies to be around €10 billion of revenues as a result of a shortage of IT specialists. Strategies such as up- or re-skilling by offering training to employees are far from common practice in SMEs. Less than 10% of SMEs provide training to ICT specialists and less than one in five SMEs offers training to other employees. Currently, more than 90% of European SMEs consider themselves lagging behind in digital innovation.

The Commission has identified IoT, big data and cybersecurity as areas where European SMEs would benefit from an increase in the skills level. Both IoT and big data hold enormous potential to maximise customer intelligence, optimise internal processes, renew business models and develop innovative services and solutions. In times where SMEs are increasingly targeted by cyber-attacks, cybersecurity is essential to ensure business continuity and protect the value chain that SMEs are part of.

A strategy that enables technology adoption and skills development

Ambitious skills policies and well-targeted supporting measures are thus needed to facilitate the access of SMEs to Europe's digital talent pool. After thorough stakeholder consultation, **this initiative brought forward a strategy** for supporting SMEs in their skills development to adopt new technologies such as cybersecurity, big data and IoT.

Designing solutions to solve the skills gap at all levels requires an understanding of both why and how an organisation adopts technology as business opportunity, and the required human capital to deliver on that investment. A study for the European Commission showed that digital transformation is enabled by strong IT competences and professionalism at the individual and team level, and digital organisational capabilities at enterprise level. It is about investing in building a capability at the organisational level, and consequently finding the right people to build competences necessary for that capability. Employees fulfil roles associated with those competences, using methods and tools to add specific value. The developed **digital capability reference framework** could help SMEs to better understand - when deciding to invest in certain capabilities - what they need in terms of competences development and provides an overview of the relevant frameworks (and related certification) for selection.

SMEs using technologies tend to perceive cybersecurity as 'some operational IT function' rather than as a core part of their digital strategy. Other SMEs find it difficult to grasp the potential that big data and IoT offer to their business. For these SMEs, awareness of business opportunities and the translation of this awareness into a clear business case could be a start to their digital transformation journey. This journey could subsequently lead them to accurately plan and implement digitalisation measures as well as facilitating a proper understanding of what concrete skills are needed to deliver on that promise. Digital SMEs might be more advanced and already have a clear understanding of which skills they require and how these skills contribute to the functioning of their business model. They still compete with large enterprises on a tight job market, which hinders growth. SMEs need a strategy on developing those digital skills in their organisation.

Moreover, especially for non-tech SMEs the potential of SME intermediaries (such as accountants, insurance experts) in bringing digital know-how into SMEs should be tapped into. SME intermediaries (clusters, sectoral associations, chambers of commerce, accountants, insurances, etc), are particularly important in building up the scale and reach of digitalisation in non-tech SMEs as they are in regular contact with SMEs, understand the underlying businesses and through their wide SME client base have broad experience in what works (or does not) particularly well in different kinds of SMEs.

"This initiative is very welcome as Europe needs to both support the SME community to become more cyber resilient as well as to facilitate growth of the widely increasing number of SMEs delivering cyber security services."

Luigi Rebuffi, CEO and founder of the European Cyber Security Organisation (ECSO)

Joint leadership to strengthen Europe's digital sovereignty

To keep Europe competitive on a global stage, and to create a strong and vital SME landscape, there is a clear need for leadership to guide European SMEs in their progressive acquisition of strategic digital skills. This endeavour will strengthen Europe's digital sovereignty and stimulate triple-helix collaboration to achieve better tailoring of education and training.

Such leadership should enable an increased adoption of cybersecurity, big data, and IoT by European SMEs via supporting measures that strengthen ecosystems and structurally enhance the supply of necessary skills and facilitate organisational development. We envision a "**European Skills for SMEs Partnership**" (Skills4SMEs Partnership) consisting of private and public stakeholders to provide the necessary strategic leadership. The aim of the **European Skills for SMEs Partnership** is to focus on measures, which can be put into **action at EU level**, while taking into account the wider digital strategy of the EU. This way, the partnership could go beyond the focus on IoT, big data and cybersecurity skills that was present in this initiative.

"Europe needs leadership to guide SMEs in their acquisition of strategic digital skills. We envision a "European Skills-for-SMEs Partnership" consisting of private and public stakeholders to provide this necessary strategic leadership."

Oliver Grün, President BITMi & European DIGITAL SME Alliance

An evidence-based roadmap to deliver the ambition

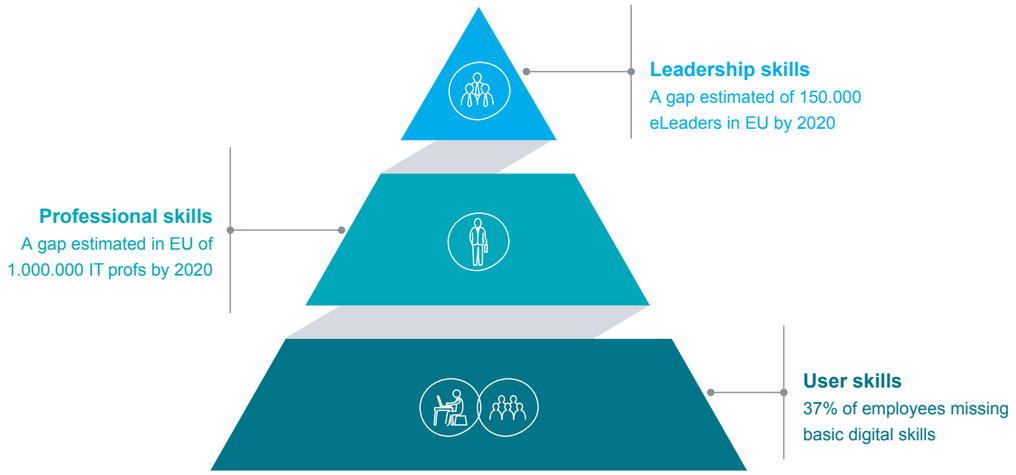
The vision is operationalised in a roadmap[1] with supporting measures targeting both the European as well as the national, regional and local levels. This plan builds on good practices identified across Europe (see an overview of these in chapter 5) and rests on three evidence-based principles:

- **Industry-led**: effective workforce development requires a good understanding of the needs of those it addresses: the small- and medium-sized enterprises. Via collaboration and participation, intelligence can be gathered on the actual needs of the companies to feed into and accelerate policy and education initiatives. A closer connection to enterprises and their owners will contribute to increased awareness since information and skills on new technologies can also travel along the supply chains and via B2B relationships.
- **Tailored and innovative education and training**: offerings need to be tailored to make them useful for SMEs. This requires innovation of current approaches: modular, blended courses, targeted at SMEs in their specific sector and geography, delivered with flexible timing, featuring practical content to enable direct action of the SME enterprise. Since technology adoption is a strategic choice, training should be fine-tuned towards the ICT professional in SMEs that have one, SME intermediaries as well as the leadership/management. Co-creation is another element of this principle.
- **Government (co-)funded and data-driven**: upskilling and reskilling of the workforce requires a strong commitment of the public sector to invest in new initiatives and to ensure the continuity of existing successful initiatives. Good practices have shown that SMEs need to contribute on the operational level (e.g. when taking courses, via cost-sharing models), but the overall strategy will require substantial public investment. A proper monitoring of how the money spent yields results, combined with research to monitor trends in industry needs, should allow to efficiently and effectively invest and feed into education and training offerings.

"At Skillnet Ireland we are committed to enterprise-led workforce development. We are positioning Ireland for the future of work by leading cutting-edge collaborations, working with more businesses and equipping people with 21st-century skills. Effective workforce development requires a good understanding of the needs of the SMEs. Our vision strongly aligns with the European Skills Strategies and we're proud to have contributed to its development."

Paul Healy, Chief Executive Skillnet Ireland

Figure 2. Skills gaps related to roles in a SME



In line with the overall rationale to enhance 'digital sovereignty', i.e. to reach a certain level of autonomy in ICT related technologies which would allow the EU to independently pursue its own interests, there is a need to enhance the uptake of skills that allow SMEs to autonomously handle technology. Consequently, this would require the development of specialist skills in the identified areas (cybersecurity, IoT and big data) and beyond (e.g. AI, quantum computing, blockchain, critical chip technologies). To develop this capacity in a sustainable manner, it is necessary to strengthen monitoring and foresight (see Pillar II of the Partnership), and to build EU skills leadership in areas that are considered vital to the economy. It seems reasonable to build on areas where Europe already has a competitive advantage and which would, at the same time, advance the goal of greater "digital autonomy/sovereignty", e.g. in Open Source software development or distributed ledger technologies/blockchain. Education and training schemes developed to that end need to be of high quality (to meet the conditions for a quality label, see Pillar I) and make sure that they do not only help SMEs gain skills in using certain ICT tools, but enhance their digital autonomy by increasing ICT specialist skills. The aim is to not just train a wide range of SME employees, but to digitise the economy via a highly skilled workforce in SMEs.

"Baden-Wuerttemberg is in the midst of the transition to digital, and exchanges in strategy dialogues with all players in the economy– such as this initiative - help understanding and developing the right measures. We invite all other EU regions to connect and create necessary synergies in knowledge and infrastructures so that we can join our forces for a sustainable and value based economy and society."

Dr. Petra Püchner, European Commissioner of Baden-Wuerttemberg and head of the Steinbeis Europe Center

A European Skills for SMEs strategy to focus on growth

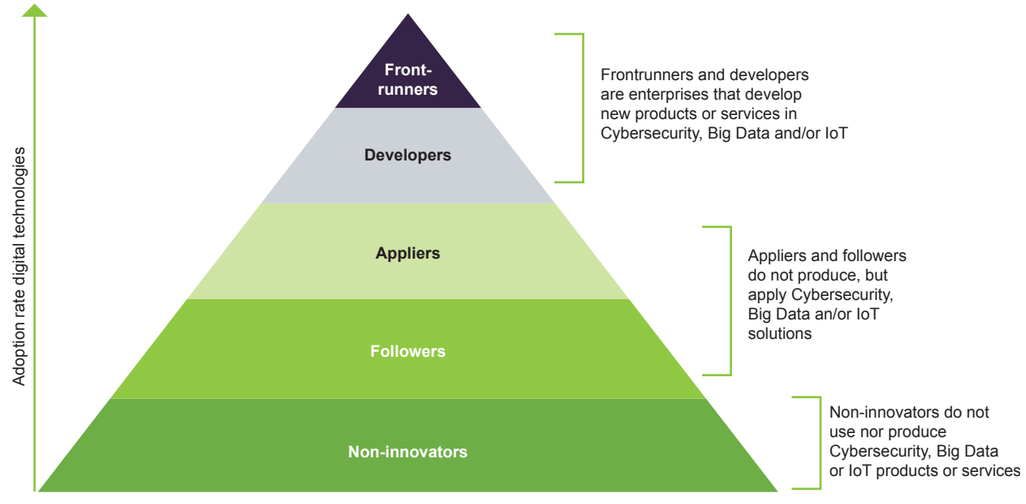
At the same time, policymakers need to be aware that measures need to be tailored to the different types of SMEs, which can be roughly categorised according to maturity and size. Maturity (as displayed in figure below): front-runners and developers, appliers and followers, non-innovators (in terms of maturity). Regarding size it is important to distinct between micro SMEs (up to 10 employees), small enterprises (up to 50 employees), and medium-sized com-

panies (50-250 employees). While it will be pivotal for nearly all businesses to digitalise in the short to medium-term (at least to a certain degree), an EU-driven strategy needs to focus on those aforementioned SMEs, where it will be most beneficial, effective, and have the greatest impact on driving competitiveness and growth. It should also contribute to the development of EU technological/digital sovereignty. Therefore, the European Skills for SMEs Partnership should focus on those SMEs in all sectors, not only the ICT sector, that have a propensity to grow, to digitalise and internationalise their business to make use of the EU internal market. The main targets are thus "**followers & appliers**" and "**frontrunner & developer**" SMEs.

"IT-using SMEs, and in particular smaller SMEs, need clear and concise support to adopt new technologies and to upskill their employees to match market demand. European collaboration is essential to share good practice with the aim to scale-up existing training initiatives and innovative approaches, and to develop products such as quality labels to increase transparency for SMEs."

Stefan Schumacher, Head of Berlin office, VOICE e.V. (German association of IT-using SMEs)

Figure 3. Segmentation of SMEs based on maturity in the uptake of big data, IoT and cybersecurity



The European Skills for SMEs (Skills4SMEs) Partnership

This proposal sets out the different recommended actions of the Skills4SMEs Partnership by grouping them into four pillars. The actions build on the principles set out above, i.e. the Partnership needs to be industry-led, data-driven and provide a knowledge-sharing platform on how to develop tailored, innovative education and training to SMEs.

Figure 4 Skills4SMEs Partnership

Skills4SMEs Partnership

Consisting of key partners in the ecosystem: Industry (SMEs and large companies), intermediaries (clusters, sectoral associations, chambers of commerce, accountants, insurances, etc), education providers, public administrations

Training and education platform	Gather intelligence and develop foresight	Strengthen ecosystem leadership	Support EU digital sovereignty
■ Grow a business support and advice funtion to strenghten single point of access: e.g. tools that clarify the business case to illustrate ROI of skills investment, practical frameworks and tools that support SMEs to build a smart (HR) strategy; self-assessments; funding information ■ Develop quality labels for training schemes ■ Procure strategic courses & develop sectoral schemes ■ Enable scaling and Internationalisation of training programmes ■ Develop concepts to support mobility of scarce expertise & train the trainer	■ Monitor skills development & forecast skills needs/supply ■ Reserch & promote data-driven approaches in SME support programmes ■ Research the motives of SMES to participate in training	■ Activate ecosystem leadership to promote strategies and best practices ■ Develop & coordinate SME training & business support accounts ■ Mapping of ecosystems: research capacities and state of play ■ Provide funding to ecosystem and SME community to provide local support to SMEs and finance expert exchanges ■ Develop common criteria of best practices to develop blueprints of successful private/public collaboration that can be scaled up in other countries/regions	■ Source talent and bring together SMEs/industry/education for support of SME strategic projects (e.g. European Cloud) ■ Support matchmaking between SMEs to pool talent for creation of innovative services ■ Further open-source-based technologies and skills ■ Continue to invest in infrastructure that enables technology adoption ■ Invest in facilities to support training programmes

We propose to develop a **European Skills4SMEs Partnership** that is dedicated to building a stronger alliance between the public and the private sector to offer leadership and a vision for skills development for SMEs in Europe. The Partnership should be accompanied with dedicated investments that enable a **long-term, strategic approach** and reduce uncertainties by allowing for long-term commitments.

The platform should drive and coordinate the following pivotal measures aimed at achieving the projected vision in the period up to 2030:

1. **Training & education platform**. This platform will be the **single access point to information** about SME skills development at EU level. It targets the intermediaries that are engaged to support SMEs directly. The platform will provide and promote quality labels on selected training schemes and give SMEs and individuals throughout Europe access to those courses. The platform also needs to develop a proactive business support function where **intermediaries** can find tools, practical frameworks, assessments, funding schemes etc. that they can bring to their local SME communities and which will also be promoted across Europe by a dissemination campaign. It will support the scaling and internationalisation of selected courses by providing translations and promoting them on a European level.
   - Enable scaling up of successful training programmes, from basic translation to providing methods or blueprints for developing successful training programmes
   - Grow a business support and advice function on the platform: e.g. offer tools that clarify the business case to illustrate ROI of skills investment, publish (links to) practical frameworks and tools that support SMEs to build a smart (HR) strategy; offer self-assessments for SMEs in specific technology domains; provide information on funding for trainings. It should

be accessible for and promoted/pushed towards intermediaries
- Develop quality labels of European training schemes based on quality criteria and standards (e.g. e-CF) and mapping according to strategic skills priorities from Pillar II "Intelligence" to increase transparency and trust as well as overall quality
- Develop concepts and practical examples to support the mobility of scarce expertise (within the education & training systems and between industry and the education & training systems). Invest in "Train the trainers" by encouraging and providing funding for the upskilling of SME intermediaries who play a role in educating and safeguarding the quality of SME-supporting professionals in the wider SME ecosystem
- Procure strategic courses and/or develop sectoral schemes that can benefit SMEs across Europe; ideally courses or schemes tailored to the needs of a specific sector (building on the Blueprint projects) or technology

2. **Intelligence & monitoring**. This task of the partnership aims to gather insights that establish a coherent, clear picture of the needs of SMEs and the supply of training and skills on the market. It should apply the methodology to forecast future developments around supply and demand of skills for SMEs. It should also take stock and research data-driven approaches at the national level to increase insights into demand/supply at an aggregated level.
   - Monitor SMEs' skills development and develop foresight on skills needs and supply
   - Promote data-driven approaches in SME support programmes
   - Research the motives of SMEs to participate in training

3. **Ecosystem[2] leadership**. Measures consisting of strengthening and facilitating the ecosystem and aimed at involving all relevant stakeholders in the partnership. This would include developing a joint approach with triple helix actors (policy, education, and industry associations) but also with accountants and insurance providers. It would require building strong partnerships at the European and national level. It proposes to develop SME training & business support accounts in collaboration with national administrations and the ecosystem, considering the national contexts.
   - Activate ecosystem leadership to promote strategies and best practices to raise awareness of SMEs for technology adoption, e.g. via their B2B environment and supply chains
   - Research the potential of SME training & business support schemes that would allow SMEs to invest in training
   - Mapping of ecosystems: research capacities and state of play, and connect to parallel initiatives at EU level to create synergies
   - Provide funding to ecosystem and SME community to provide local support to SMEs and finance expert exchanges
   - Develop common criteria of best practices to develop blueprints of successful private/public collaboration that can be scaled up in other countries/regions

4. **Support EU Digital Sovereignty**. Build on ICT industry frontrunners to strengthen SME skills and develop leadership in strategic areas by bringing together larger companies, SMEs, and research and education. Based on the strategic priorities identified in Pillar II "Intelligence", this pillar aims to stimulate the collaboration of innovative SMEs with industry and academia to engage in consortia for innovation projects. The actions and measures could build on the strong open source community to further skills in developing an ecosystem of non-proprietary software and related skills.
   - Source talent and bring together SMEs/industry/education to support strategic projects (e.g. European Cloud, blockchain, AI, open source software)
   - Support matchmaking between SMEs to pool talent for the creation of innovative services[3]
   - Promote open source-based technologies and skills
   - Continue to invest in infrastructure that enables technology adoption
   - Invest in facilities to support training programmes

Required investments at national and EU level

The actions at EU level refer to initiating and intensifying collaboration, knowledge sharing, and providing tools at EU level that support the creation of a common European language and will require funding to initiate this development. The countries, and various stakeholders in those countries, can benefit from the actions deployed here. However, they will have to deploy their own national and/or regional skills strategies, and especially start to plan for investing in skills development schemes that are pivotal to support SMEs in their digital transformation. This requires a long-term and dedicated investment.

> ***"Digital transformation is a big challenge for SMEs and we need a comprehensive and coherent approach in Europe and Member States to enable and facilitate SMEs to adopt new technologies. Skills development for entrepreneurs and workers is an essential part of that, particularly through Vocational Education and Training (VET) including apprenticeships."***
>
> Véronique Willems, Secretary General of SMEunited

An essential element in advancing skills development in SMEs is the **scaling of existing good practices in learning programmes**. A recent study for the European Commission analysed the funding models of education and training programmes targeting the workforce at national and EU level to understand how successful initiatives can be scaled up to increase impact. Practices that have proven their value and address a strong stakeholder demand need - deserve! - scaling to increase impact. The study comes forward with recommendations in five areas: vision & long-term strategy, scalable multi-stage funding intervention, massive investments & new ways of funding, means to guide future policy development, and high-tech skills hubs to connect key actors.

"In collaboration with the European Commission, the OECD Digital for SMEs Global Initiative (D4SME) intends to promote knowledge sharing and learnings on how different types of SMEs can seize the benefits of digitalisation, and on the role of government, regulators, business sectors and other institutions in supporting SME digitalisation. We need urgent action, for instance on cybersecurity as only 46% of governments have a specific strategy and actions plans in place."

Marco Bianchini, Policy analyst, Centre for Entrepreneurship, SMEs, Regions and Cities, OECD

Investments needed in skills strategies are indeed massive but essential to advance. To give an order of magnitude of what is needed: according to add statistics, only 32% of European SMEs had a formally defined ICT security policy in place. This means approximately 17 million SMEs did not and will have to acquire these skills by investing in training courses to develop that knowledge in-house or hire it externally. In similar fashion, statistics reveal that only 12% of SMEs were using some type of big data source, compared to 33% of large enterprises. Closing that gap would require to reach at least five million SMEs. From good practices, it becomes apparent that co-funding or cost-sharing models are most effective. Good practices across Europe reveal current levels of investments at different government levels:

- **Skillnet Ireland** runs a budget of €35.9 million for 2020, with the total investment in upskilling by Skillnet Ireland likely to exceed €60 million when employers' contributions are added. Skillnet Ireland works in partnership with 50 industry bodies and enterprise clusters, providing training and innovation support to over 16,000 businesses, and they upskill 56,000 workers throughout the country every year.
- The **German Federal Ministry for Economic Affairs and Energy** (BMWi) launched a funding programme called 'Go-Digital' of €7.2 million (in 2 phases) which enables nearly 700 projects. The subsidy voucher system that activates skills development in SMEs via external consultants has been successful and revealed an appetite for further expansion of this scheme.
- The **JADS SME Data-lab** is an excellent local example from Den Bosch (NL), which helps SMEs to create value with data. Over 100 SMEs entered the lab to come out with a proof-of-concept or tailor-made solution that helped them reduce costs or increase revenues. There is a standard fee of €2500 and half of the money goes to the data science students that JADS staffs on these projects.

However, more dedicated funding schemes for skills development in SMEs are needed across Europe to increase technology adoption and close current skills shortages in SMEs. Part of this could come from EU funding, but most of this amount will be an investment by national, regional and local entities aiming to boost competitiveness of SMEs and drive their economies forward.

Further investments would be needed at EU level to secure the development of the proposed Skills4SMEs platform and partnership, including the proposed measures to develop quality labels, concepts for scaling good practice of learning programmes and funding models, to monitor SMEs' skills development and develop foresight on skills needs and supply, to activate ecosystem leadership, and to support matchmaking between SMEs to pool talent for the creation of innovative services.

The 'blueprint for sectoral cooperation on skills' is one of the key initiatives of the skills agenda for Europe, investing €28 million of funding in 2018 and launching new sectors yearly. Recently, a new chapter was launched that addresses the cybersecurity, software and blockchain sector, among others.

Another initiative to start in 2020 is the European Digital Academy. The overall objective of the European Digital Academy is to contribute to the development, reskilling and upskilling of European citizens and SMEs on some of the key emerging technologies (AI, Blockchain, robotics, cybersecurity, IoT). It will be done by developing a new platform closely connected to the European Portal for Digital Skills and Jobs. The platform will map the online learning opportunities from different providers in an easy-to-access manner. In addition, modern and highly engaging online training modules will be developed based on the needs identified by the project.

Further investments would be needed at the national level (including regions and cities) to invest in skills development for all relevant digital areas (not only cybersecurity), to push for change in education and training systems to become more adaptive to new demands, and to mobilise expertise with relevant intermediaries in regions and cities to increase engagement of SMEs in digital transformation and corresponding skilling activities.

"Cities are enablers of SME growth. We believe our city of Helsinki is a platform for SMEs to grow and flourish, even beyond our city borders. It requires competence development and capacity building as well as strengthening the ecosystem. Collaboration, joint development and innovation are pivotal."

Sanna-Mari Jäntti, Director Strategic Projects, City of Helsinki

VISION STATEMENT

Enabling an increased adoption of cybersecurity, big data, and internet of things by European SMEs via supporting measures that strengthen ecosystems and structurally enhance the supply of necessary skills and facilitate organisational development.

The urgency of supporting SMEs to become cyber resilient

Cybersecurity composes real threats for SMEs...

The emergence of new technologies brings new opportunities for enhanced business performance and operations, but also introduces several information security and privacy risks. Since the beginning of 2016, more than 4,000 ransomware attacks occurred worldwide daily. This is an increase of 300% since 2015. Speaking about cyber incidents in general, **around 80% of companies in Europe have experienced at least one cybersecurity incident** in 2016[4].

The costs of cybercrime for those impacted are high and growing. **Estimates show that the annual global costs of cybercrime will grow to around 4.8 trillion EUR by 2021**[5]. However, the reputational damage for affected companies is often even bigger than the direct monetary damage[6].

Not only big companies, but also **SMEs fall victim to cyber threats more and more often**[7]. Although many owners of SMEs underestimate their risk of becoming the target of a cyber-attack, they are likely targets for cyber criminals[8] or state-sponsored attacks[9]. Today, **SMEs are increasingly dependent on their information systems and networks** to provide services and products and meet their business objectives. The vast majority of SMEs (excluding micro-enterprises) rely on some form of information system and many of them already have an online presence. Electronic communication networks, interconnected information systems and digital services are an essential part of an increasing number of SMEs[10].

What also makes SMEs vulnerable is that they generally have relatively many different digital assets per individual user, their security is limited compared to bigger companies and they generally are less careful to prevent cyber-attacks[11]. Now that most large businesses have dedicated cybersecurity teams, cyber criminals increasingly target smaller enterprises. Perhaps SMEs are even a more likely target than large corporates, as due to a perceived lack of security, **cyber criminals are increasingly looking towards SMEs as a gateway into the supply chain**[12].
More and more SMEs report to be victim of digital fraud causing financial damage. Especially for SMEs, this financial damage can have a profound impact: one research indicated that 60% of SMEs that were victims of cyberattacks did not recover and had to shut down within six months[13].

... but it also offers opportunities

However, cybersecurity is not only about threats. It can also be a driver for growth for companies active in the cybersecurity market. It can even bring competitive advantage according to Capgemini research. The increase in cybersecurity incidents stimulates the demand for high-quality, affordable and interoperable cybersecurity products and solutions. Cybersecurity is one of the fastest growing sectors of the ICT market. Worldwide spending on cybersecurity products and services reached more than 120 billion USD in 2017. In the last decade, the market was growing 8-10% annually, while predictions for 2017-2020 envisage further steady growth[14]. This number is estimated to exceed 0.8 trillion EUR cumulatively over the next years until 2022[15]. In Europe specifically, the cybersecurity market is estimated to grow from 21.8 billion EUR in 2015 to 30.6 billion EUR in 2020[16].

European policymakers recognising the need to act

Cybersecurity was a central element in the 2018 State of the Union speech by the EC President[17]. One of the proposals included the creation of a Network of Cybersecurity Competence Centres, coordinated by a new European Cybersecurity Industrial, Technology and Research Competence Centre. Leveraging the already existing 660 cybersecurity centres across the EU, this new initiative seeks to:

- Pool, share and ensure access to existing expertise;
- Help deploy EU cybersecurity products and solutions;
- Ensure long-term strategic cooperation between industries, research communities and governments;
- Co-invest and share costly infrastructure.

The European Union works on a number of fronts to promote cyber resilience.

> ***"This and many other initiatives to promote cyber resilience and increase awareness and skills for SMEs are of the utmost importance as a stable long-term strategic collaboration between the relevant actors. It is essential also to stay ahead in the game with cyber criminals increasingly targeting SMEs as a gateway into the value chain and the entire digital ecosystem."***
>
> George Sharkov, Adviser to the Minister of Defense in Bulgaria, Director ESI CEE, Member of the High-Level Expert Group on AI

The huge potential of adopting Big Data and IoT for SMEs

Equipping European SMEs with the means and tools to mine, process, store and analyse big data and generate value from it "is a means of securing future wealth and prosperity"[18]. Data holds an enormous potential in various fields, such as health, food security, climate and resource efficiency to energy, intelligent transport systems and smart cities - and is considered "an essential resource for economic growth, job creation and societal progress"[19]. An EU publication on the data economy righteously states that "companies can use big data analytics to help them develop new products and services, to re-engineer their business processes and better manage their supply chains, to strengthen fraud detection, to improve security and risk management and to gain clearer insights into customer needs" . An advantage that SMEs have in this regard, because of their size, is that they tend to be more flexible in using the insights generated from big data in order to increase sales, reduce costs, improve customer satisfaction, increase productivity and accelerate innovation.

The 2017 European Data Market [20] study showed that the data economy is already a reality today. Approximately 6.1 million EU citizens could be considered 'data workers' in 2016, and this number grows with around 2 to 3% per year, faster than average, potentially rising up to 10.4 million by 2020. Furthermore, these are not merely ICT jobs as might be expected: the ICT industry accounts for only around 11% of data workers, as opposed to professional services (20%), wholesale and retail (18%), and manufacturing (12%). The distribution of these jobs shows that the economy is increasingly becoming data-driven, including in sectors that are more traditional.

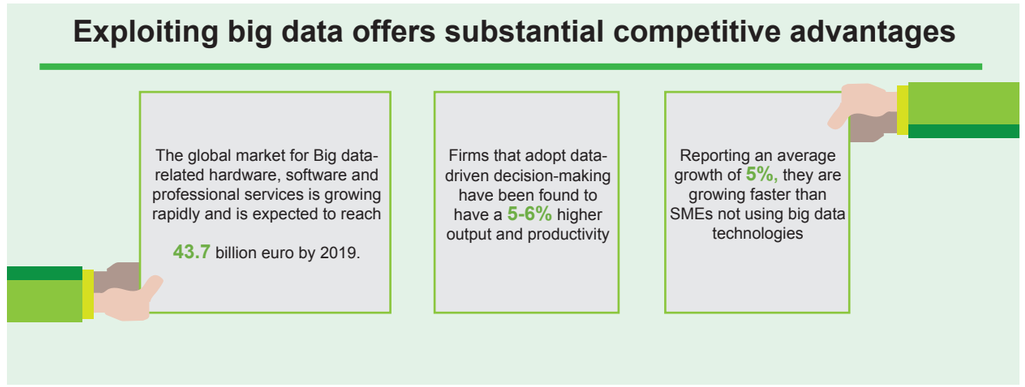
Nonetheless, there is a margin for improvement: only 661,000 enterprises in 2016, corresponding to 6.4% of the 10.3 million potential user companies (excluding the government sector) can be characterised as data-driven users. This is relatively modest and shows that significant gains are still possible. Under high growth scenarios, an increase to around 359,000 companies by 2020 should be viable.

Increasingly, companies have understood the potential benefits and are investing rapidly in big data technologies and services. However, not all companies have equal opportunities to reap the benefits of the emerging data market. Access to data and the ability to exploit the value are key. With limited access to data and data analytics, European companies will not be able to compete in global markets and SMEs and emerging companies are the ones set to lose the most[21].

"The BDVA is keen to support SMEs to become more data-savvy and enabling them to benefit from big data and data analytics. In particular, it is important to look into the recognition of skills acquired through informal learning as it can help employees grow a career faster and employers to understand the competences they have in-house."

Ernestina Menasalvas, Professor University of Madrid, Lead of Big Data Value Association Task Force 9: Skills and Education

The promise and potential of IoT is substantial. The worldwide IoT market is expected to grow to more than 7 trillion dollars by 2020[22]. At the same time, the development of the IoT market has only recently started. In 2015, of all physical objects that can be connected to the Internet, less than 1% actually were connected. This means that just under 15 billion of the approximately 1.5 trillion items on earth were connected to the Internet at that time. This number is expected to increase up to level of more than 50 billion devices connected to the Internet by 2020[23]. Specifically, for the EU28, IDC expects the number of IoT connections to grow to a level of almost 6 billion in 2020, and revenues growing up to a level of 1,181 billion EUR in 2020[24]. Within the EU, the number of IoT connections is expected to increase from 1.8 million in 2013 to almost 6 billion in 2020, which means the IoT market will be worth more than one trillion dollars by then[25].



The growth in connectivity is expected to bring economic benefits, with IoT reshaping and transforming existing industrial structures. Borders between products and services, as well as borders between industries will become less obvious than today. This may materialise in innovative IoT services or applications, improved products, more efficient processes and a reduced consumption of resources and a better understanding of customers' needs.

It is important to note that one can distinguish benefits for users and benefits for suppliers. Much of the IoT market is based on business-to-business interactions, meaning that ICT vendors provide IoT technologies and solutions to business users, who leverage them to deliver services and applications to their customers. A group of so-called enabling companies play an important role in the IoT ecosystem, referring to big data companies, security providers, application developers, and other professional services companies[26].

Risks have also been signalled as the market of IoT devices is increasingly price-competitive meaning that producers of IoT devices have to produce at lower costs which can influence the quality of the product. This can impact for instance the security of the device.

The potential of IoT is huge, but several studies point to the fact that many businesses are still in the early stages of IoT adoption, where its use is limited to a single business function, rather than being committed to a formal business–wide program[27]. As regard the role of SMEs in IoT adoption, the report 'Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination'[28] states that SMEs play a relevant role in the development of the emerging IoT combined ecosystems and their diffusion. They mainly refer to the role SMEs can have in the supply ecosystem, and state that SMEs currently have insufficient capability to enter this market. One of the recommendations is to increase their capability, and to facilitate their access to the necessary technology platforms to develop applications and services. SMEs are primarily active in the group of ICT vendors - providing components to solution providers. Examples include systems integrators, hard- and software providers and cloud service providers. The role of SMEs within this IoT ecosystem can be more substantial, adopting IoT on a larger scale. Several factors are preventing SMEs from doing so: insufficient investments and organisational barriers to change, concerns about privacy and data protection, mismanagement of security risks, and a lack of standards and interoperability across fragmented European markets preventing economies of scale and scope[29].

A thorough assessment of barriers hindering SMEs in adopting new technology

Barriers in big data adoption

There are various factors that condition the poor adoption of business and big data analytics by SMEs, such as cultural barriers, shortage of affordable consulting and business analytics services, a non-transparent software market, a lack of intuitive software, and financial barriers. Specifically, to people and skills four barriers stick out[30]:

1. **Dominance of domain specialists**. As operating in a niche or specialised field is a strength of SMEs, the major part of the employees are domain specialists, with more generic functions poorly covered. This is not beneficial for spotting new business opportunities and trends outside of the respective domain, such as big data analytics.
2. **Shortage of in-house data analytic expertise**. SMEs lack own employees with data analytics capabilities. Several factors play a role here[31]:
   a. High set-up costs, combined with uncertainty about future return on investments;
   b. Lack of management expertise to set up and embed a data analytics unit;
   c. Shortage of qualified workers and excessive staffing costs.
3. **Bottlenecks in the labour market**. There is a growing shortage of qualified data analysts on the labour market. IDC studied the European data landscape, and forecasts that the structural imbalance between demand and supply will result in a data skills gap in 2020[32].
4. **Lack of understanding**. A recent e-Skills survey in the UK[33] highlights an extremely low understanding of big data analytics by SME representatives, whereas among larger organisations, around 30% to 40% claim to have good or very good understanding of big data analytics. A recent Germany survey[34] portrayed a similar picture, with around 30% of respondents considering their big data knowledge to be good or very good.

Barriers in IoT adoption

The potential of IoT often is not realised. There are a number of reasons for this, of which security concerns and constrained analytical capabilities are amongst the most pressing barriers[35]. For IoT, SMEs need strong technological competences[36]. First, sensors increasingly generate huge volumes of data at a real-time basis. Companies would need a robust analytics platform to benefit from the growing volumes of structured and unstructured data - including the ability to 'clean' the unstructured data. Second, they need advanced analytics, and increasingly AI capabilities, ranging from descriptive to prescriptive analytics. Descriptive analytics are used to gain a granular view of the specific process that is being measured and monitored, and prescriptive analytics and AI to learn from past patterns and to anticipate on future developments. Third, the adoption of a 'security-by-design' approach is crucial to address cybersecurity threats.

It is stated [37] that ensuring SMEs' capability to enter the IoT market is a key challenge. Various obstacles need to be overcome: insufficient investments, organisational barriers to change, concerns about privacy and data protection, mismanagement of new security risk, and a lack of standards and interoperability across fragmented European markets - preventing economies of scale. Other barriers identified[38] include the lack of a convincing business case, security concerns and risks associated with change. A lack of qualified personnel is also among the barriers, and refers not only to the technical perspective, but also to difficulties with evaluating the value capture of IoT. The Internet of Things Business Index[39] highlighted a lack of IoT skills and knowledge as one of the top-three barriers holding businesses back from adopting IoT.

Barriers in cybersecurity adoption

There are various specific barriers for the adoption of cybersecurity by SMEs. This is problematic not only because SMEs are already vulnerable to cyber threats, but also because security concerns are barriers for the adoption of both big data and IoT. The use of these new technologies brings new opportunities, but also introduces information security and privacy risks. There are many dimensions to effective cybersecurity and data protection-from strategy and operations, to governance and culture-but one of the biggest problems is simply the lack of talent[40]. Those companies that attract and retain cybersecurity talent will be much more successful in managing digital risk and profiting from big data and IoT. In 2015, ENISA stated that despite rising concerns on information security risks, the level of SMEs' information security and privacy standard adoption is relatively low[41]. The report clusters the barriers that contribute to the limited uptake of cybersecurity practices by SMEs in four categories[42]:

1. **Knowledge and engagement**: awareness of standards, limited awareness of how standards add business value, prevailing perception that cyberattacks are mainly threatening large enterprises, design of standards mainly driven by larger enterprises;
2. **Capabilities and resources**: the implementation of information security and privacy standards can be demanding in terms of financial resources. For SMEs that have internalised the ICT function, often one employee is responsible for security along with his/her other ICT responsibilities, resulting in limited time and dedication for security practices. SMEs that have outsourced the ICT function may suffer from limited internal knowledge about cyber threats;
3. **Shortage of standards in specific areas**: there are limited European or international standards designed to assist small organisations towards ensuring appropriate protection of personal data;
4. **Implementation aspects**: Standards are often hard to understand for SMEs not having the inhouse expertise for translating standards into specific tasks and activities. Especially when there is a lack of clear implementation guidelines.

"According to research, the majority of small business owners don't fear a cyber attack and most of them are confident they can rebound when hit by an attack. The reality is quite the opposite! Action is required at all levels to protect the SMEs ánd the value supply chains they are part of."

Jan Wessels, Information Security Officer Rabobank

Digital transformation cannot take place without a solid cybersecurity approach. The more a company becomes dependent on ICT and the more a company embraces emerging technologies such as big data and IoT, the more crucial cybersecurity becomes. Moreover, measures aimed at addressing the barriers for cybersecurity will also positively affect the take-up of big data and IoT.

Comprehensive overview of barriers hindering skills development in SMEs

These specific barriers for skills development emphasize that skills development is not straightforward for SMEs. Participating in training courses not only depends on internal factors such as capacity and financial resources, but also on the 'fit' between SME training demands and courses available on

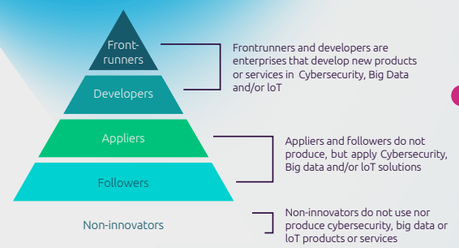
ROADMAP

Skills development for SMEs: Fostering the Adoption of Cyber-security, Big Data and IoT

START

SMEs

IT-using and producing SMEs in different stages of maturity



VISION

Enabling an increased adoption of cybersecurity, big data, and internet of things by European SMEs via supporting measures that strengthen ecosystems and structurally enhance the supply of necessary skills and facilitate organisational development.

STREAM I. STRENGHTENING ECOSYSTEMS

Being connected and embedded in regional or sectoral support structures – 'ecosystems' - is essential for SMEs' skills development. In every corner of Europe, SMEs need to be embedded in networks and have access to nearby support (knowledge, guidance and learning).

STREAM II. STRATEGIC OUTLOOK DEVELOPMENT

Aimed to increase the understanding of the strategic business opportunity of adoption of BIC. Starting with raising awareness and creating a strategic outlook. Also requiring strengthening of direct business environment and facilitation of collective action.

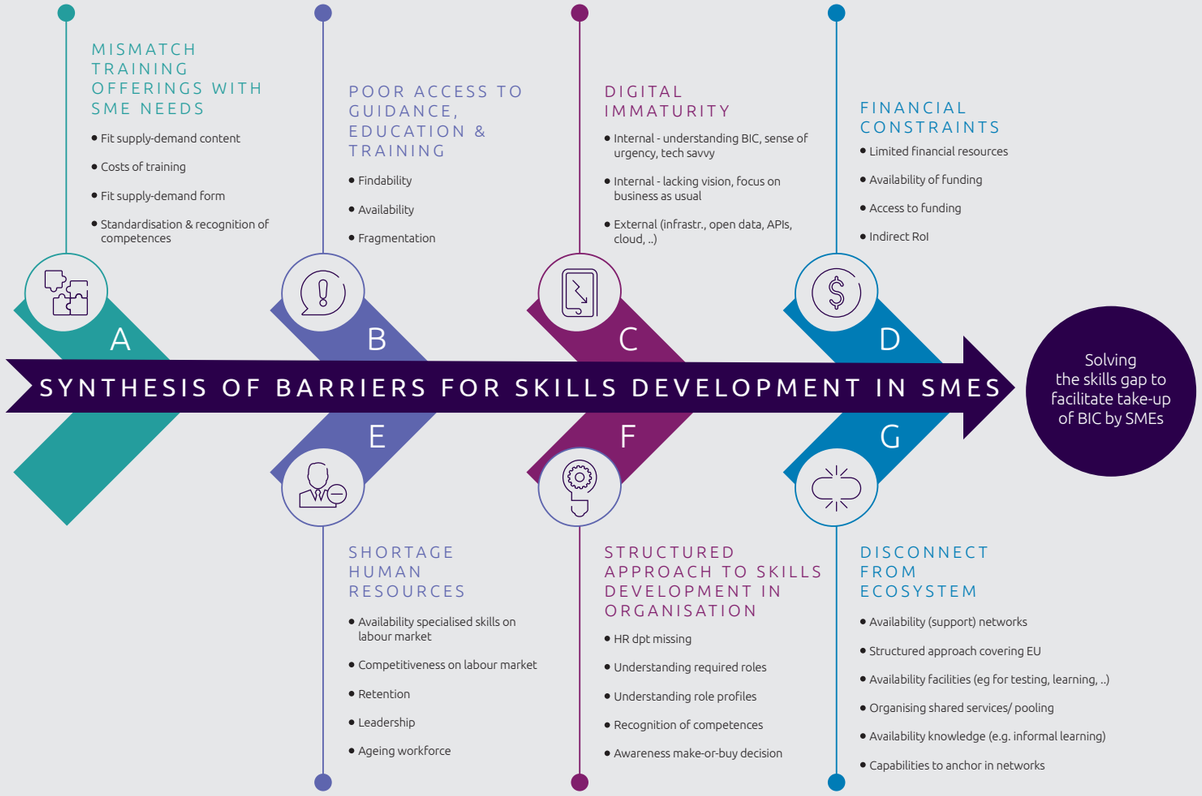
STREAM III. STRUCTURED SKILLS DEVELOPMENT

From vision to plan: support SMEs with the implementation of structured skills development, enhance capabilities for assessment, monitoring and decision-making (the business case!) & increase transparency and access to funding.

STREAM IV. TAILOR TRAINING TO SMES' NEEDS

Increase education and training offers: build sustainable training offers that match SMEs needs (content, form, set-up). Develop training capacity. Collect intelligence to increase understanding of needs. Reduce direct costs.

NEW START



EXPLANATION OF BARRIERS FOR SKILLS DEVELOPMENT

CLUSTER	EXPLANATION BARRIERS
A TRAINING OFFERINGS	• Content: Available trainings not tailored to specific needs of SMEs, e.g. too theoretical, not focusing on BIC specifically, in other languages; • Form: Trainings are delivered in formats not always suitable for SMEs, e.g. too long, during work-hours, balance online/offline, etc.; • Costs: Available trainings are often too costly for SMEs, who have to prioritise their investments because of limited financial resources;
B ACCESS TO GUIDANCE, EDUCATION & TRAINING	• Findability: If trainings, tools and information are available, they are not always findable by SMEs and not made available at 'natural' places SMEs go; • Availability: Specific trainings, tools and information in the area of BIC technologies are not always available for SMEs; • Fragmentation: Guidance & training is sometimes available, but highly fragmented across Europe: in some regions, extensive support structures exist whereas in other regions hardly any information, tooling, training or other support is available.
C TECH MATURITY	• Internal – tech savvy: A lack of tech savviness of SME manager/owners leads to manager/owners not understanding the value of BIC technologies, or not recognising the sense of urgency to adopt BIC. Lack of tech savviness also contributes to managers/owners not knowing what types of products and services are appropriate to buy for their business. The lack of standards makes this even more complicated. It also makes SMEs dependent; • Internal – operational focus: Too often, SMEs focus on the short term, on business as usual, and lack a long-term vision (e.g. on technology); • External infrastructure: An external infrastructure focusing on the take up of emerging technologies (e.g. open data, APIs, open source solutions) might incentivize SMEs to develop the skills needed to adopt BIC. • Dependency on external contractor: Less capacity to test and try out (linked to general financial risk above) and less know-how on negotiation of contract terms for service level agreements, thus a higher risk of agreeing to unfavourable or unnecessary ones.
D FINANCIAL RESOURCES	• Limited financial resources: It is difficult for SMEs to find the financial resources needed to offer training to their employees; • Availability of funding: Support in the form of funding has proven to be effective (e.g. Skillnet IE), but is not equally available throughout the EU; • Access to funding: If funding is available, SMEs might not be aware or do not know how to get access to funding. Being connected or embedded in networks facilitates access to funding; • Indirect Return on Investment (ROI): SMEs have limited financial resources. The return on training investments tends to have a relatively large lag. As a result, they tend to struggle to commit to long-term financial investments, which are essential to internalise BIC technologies.

CLUSTER	EXPLANATION BARRIERS
E HUMAN RESOURCES	• Labour market: the availability of specialised BIC skills are scarce on the market; • Competitiveness on labour market: To attract talents, SMEs need to compete with big corporates who can afford higher salaries. At the same time, SMEs might benefit from 'millennials' who might appreciate the flexibility, agility and start-up culture of SMEs; • Retention: Even if one is able to attract BIC talents, retention remains a challenge in today's competitive labour market; • Leadership: The smaller a company, the more the performance of such a company is dependent on the owner or manager. The continuous development of their skills and knowledge is of crucial importance; • Greying workforce: Age management has become a challenge for companies in general, and in particular for SMEs
F AWARENESS SKILLS NEEDS	• HR department: HR processes and skills development are often not organised in a systematic way or with a long-term approach within SMEs; • Awareness roles required: Perception and awareness of roles required to build the capabilities to adopt BIC; • Awareness skills needed: Perception and awareness of competences required (training needs) per role. Standardisation of roles; • Standardisation & recognition competences: Available trainings are not part of widely accepted framework. Informal learnings processes are important for SMEs, but these learning experiences are not documented / validated; • Awareness make-or-buy decision: Difficulties with decision to internalise skills or to hire skills on the market – lack of standardisation. This creates difficulties in professional commissioning.
G ECOSYSTEM/ NETWORK	• Availability networks: The involvement in networks, cooperation or cluster activities enable SMEs to engage more effectively in ongoing training and skills development; • Structured approach: Availability of support structures throughout the EU. Currently fragmented and not coordinated at EU level; • Availability facilities: Facilities for testing and learning (e.g. incubators) are not always available; • Organising shared services: Shared services (pooling of companies) within a network can be beneficial, but can be perceived as difficult to organise; • Available knowledge: both tacit and explicit knowledge cannot always tapped in to (peers, knowledge institutes, big corporates); • Managerial capabilities: SME manager/owners need to have the capabilities to become anchored in networks/clusters/ecosystems.

Skills strategies: successful digital transformation requires systematic skill development

Successful digital transformation requires systematic skill development. There are three major drivers of skill development in firms. First, the 'deciders' or **management** should show the commitment and strategy to ensure the operationalisation of digital transformation; second, the **organisation** must ensure that digital transformation is driven by cross-functional work and there is a sufficient knowledge transfer; and third, the **culture** in the firm should stimulate discussions on digital transformation goals and skills development needs[43]. Without such a supportive environment, the integration of such technologies, as well as, development of needed skills for the uptake of these technologies is highly problematic in SMEs.

There is a variety of strategies on digital skills development; the choice of a strategy is largely determined by the digital maturity stage of SMEs, which implies the willingness of the management team to embrace changes in a firm and the assessment of the impact of technologies on business processes. The cost-benefit analysis is normally guiding the choice of a strategy and the size of investment for skills development in an SME. If a technology is at the core of all business processes, and consequently has a large value for an SME, then a company is likely to invest more resources into skills development to ensure effective operation of the technology. In such a case, the number of people who receive training to upgrade their skills is likely to be larger than if a technology has a small function in a company.

Most companies are using traditional strategies to address skills gap, either **in-house solutions** - training by colleagues or invited experts and recruitment, or **external solutions** - outsourcing of skills through partnerships with companies that possess needed skills. The choice between internal versus external skills strategy is determined by multiple factors:

- Availability of a suitable trainer and a course either within an SME or outside of it;
- Ability to train employees, complexity of training;
- Frequency of use of needed skills;
- Potential to use needed skills in other tasks;
- Risks if skills are not developed in-house;
- Ease of doing business without needed skills in-house (with partners, clients);
- Direct costs of required training versus the costs of outsourcing;
- Investment costs of current staff upskilling and a fear of them leaving the company versus the cost of finding the right provider of skills;
- Opportunity cost for not continuing business as usual.

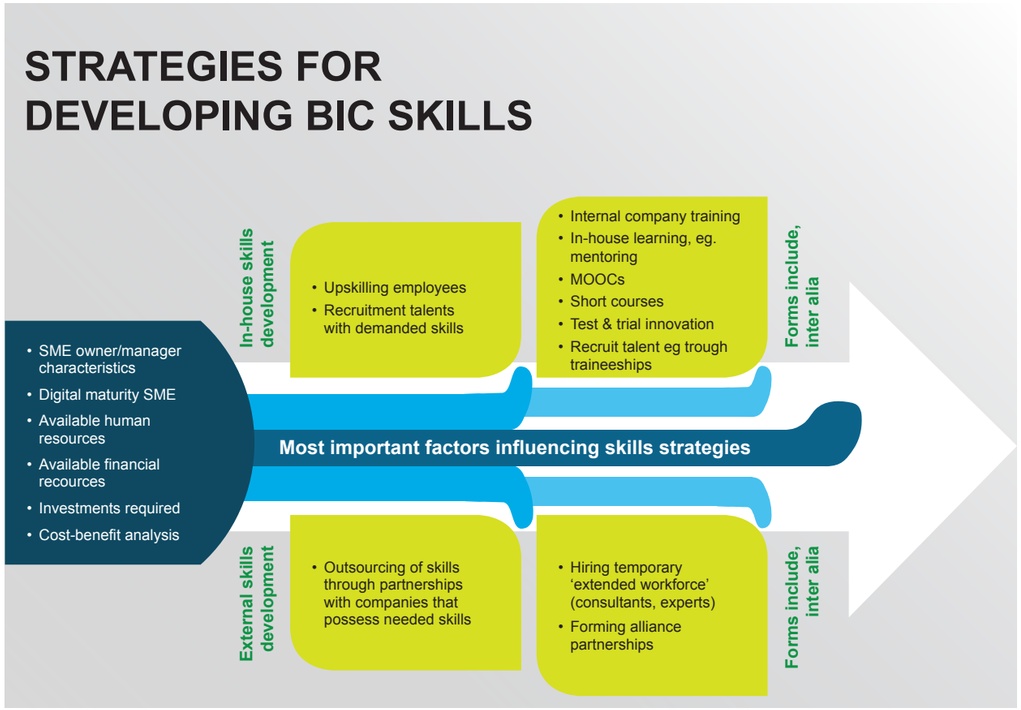
Strategies of SMEs to approach skills needed for the three technologies at hand are motivated by a wide range of company specific factors. SME managers/owners embracing digital transformation are rare but are a step ahead in their approach towards digital skills development. Hence, the stage of digital maturity is associated with the skills development strategy chosen by an SME. The lack of knowledge and skills of managers/owners in SMEs prevents them from understanding the potential of these technologies and discourages investment in digital skills development.

Traditional digital skills development strategies, such as training, recruitment and outsourcing are most popular in companies – both large and small. The choice of the right strategy for an SME depends on an assessment of needed

skills, available resources, amount of various types of investments and costs and use of acquired digital skills through cost-benefit, cost-effectiveness, efficiency and opportunity cost analyses.

"The European e-Competence Framework (e-CF) can be of great value to SMEs to enable them to create or harmonise internal job descriptions, draft vacancies, and assess or articulate competencies in a common and understandable way. The e-CF is a great support to implementing the human capital aspects of a digital strategy."

Mary Cleary, Deputy Chief Executive Officer
Irish Computer Society



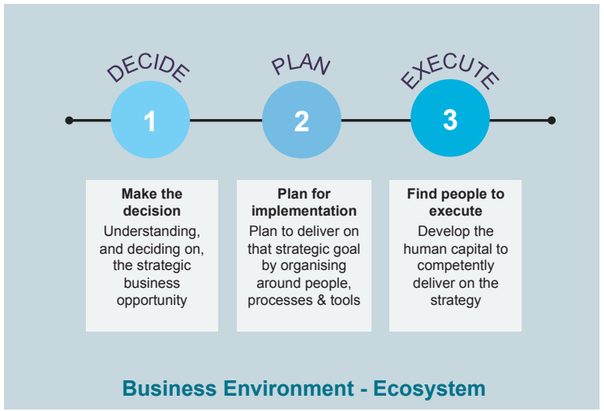
A vision to guide triple helix initiatives

The activities conducted led to the formulation of the following vision statement, which is supported and validated by a broad variety of relevant stakeholder groups[44] that were consulted in the process:

Enabling an increased adoption of cybersecurity, big data, and internet of things by European SMEs via supporting measures that strengthen ecosystems and structurally enhance the supply of necessary skills and facilitate organisational development.

In this vision statement, the following elements are important:

- **SMEs are part of a value chain of companies**, which allows them to share, collaborate, learn and grow. Measures should strengthen these ecosystems, as they are the most effective driving force of increasing the adoption of big data, internet of things and cybersecurity.
- **Advancing the digital maturity of SMEs starts with a strategy to adopt technology to create business value**: understanding the skills a company requires, starts with an understanding of how the technology contributes to the company's strategy. Measures should be aimed at increasing awareness of how to embrace and embed these technologies in the digital strategy of the enterprise, and from that direction derive the competences and roles and skills involved to deliver on that strategic objective. Measures should also include concrete tools and instruments that facilitate capability development in the organisation (especially from an HR function point of view - which is often lacking or minimally organised in SMEs).
- **Technology adoption requires the right skillset**. Measures should be aimed towards increasing the supply of the necessary skills on the labour market, via upskilling programmes of employees in the company and by increasing the number of graduates in the relevant educational fields (universities, business schools, VET).



The underlying concept builds on a previous EC study on Digital Capability Reference Framework and requires understanding the balance between an organisation's strategy on why and how to adopt technology as business opportunity, and the required human capital to deliver on that investment. It is about investing in building a capability at the organisational level, and consequently finding the right people to build competences necessary for that capability. Employees fulfil roles associated with those competences, using methods and tools to add specific value. We used this step-wise approach to structure the roadmap with supporting measures, building from the barriers analysis.

ROADMAP

In order for this vision to become effective, it needs to be operationalised and translated into concrete actions to tackle the aforementioned barriers in a coherent and consistent way. The roadmap that was developed over the course of this project addresses four streams of action:

I. **Strengthening ecosystems**: Being connected and embedded in regional or sectoral support structures - 'ecosystems' - is essential for SMEs' skills development. In every corner of Europe, SMEs need to be embedded in networks and have access to nearby support (knowledge, guidance and learning).

II. **Strategic outlook development**: Aimed to Increase the understanding of the strategic business opportunity of adoption of new technologies. Starting with raising awareness and creating a strategic outlook. Also requiring strengthening of direct business environment and facilitation of collective action.

III. **Structured skills development**: From vision to plan: support SMEs with the implementation of structured skills development, enhance capabilities for assessment, monitoring and decision-making (the business case!) & increase transparency and access to funding.

IV. **Tailoring training to SMEs' needs**: Increase education and training offers: build sustainable training offers that match SMEs needs (content, form, set-up). Develop training capacity. Collect intelligence to increase understanding of needs. Reduce direct costs.

Each stream consists of sub-goals with multiple supporting measures addressing policymakers, education providers, industry and other stakeholders such as accountants and insurance companies. The following sub-goals were identified.

I. **Strengthening ecosystems**:
   a. Gather intelligence & increase transparency: Determine the current state of play by mapping existing ecosystems, identifying their strengths & weakness and increase transparency thereof
   b. Strengthen and expand existing ecosystems & initiatives: extend and support existing networks, hubs & initiatives to reach a more comprehensive coverage which will allow access to every SME
   c. Boost the effectiveness of the overall EU, national and regional ecosystems: Stimulate knowledge exchange between ecosystems

II. **Strategic outlook development**:
   a. Raise awareness within SMEs on opportunities that technology adoption holds and threats of ignoring it for business continuity
   b. Strengthen the direct business environment of SMEs: increase strategic capacity & knowledge via stimulation of the eco-system and providing necessary infrastructure
   c. Facilitate collective action to overcome hurdles related to size and scale

III. **Structured skills development**:
   a. Support SMEs with the implementation of structured skills development
   b. Enhance capabilities for monitoring & decision-making in SMEs: via instruments that help SMEs identify the to-be situation, their current state and available solutions to bridge the gap
   c. Increase transparency and access to funding: Make sure SMEs use available resources and understand the business case

IV. **Tailoring training to SMEs' needs**:
   a. Increase education and training offers; build sustainable training offers that match SMEs needs (content, form, set-up)
   b. Develop training capacity: Increase pool of trainers/teachers and improve facilities to anticipate demand for relevant training
   c. Collect intelligence: Increase understanding of skills gaps in SMEs to better inform policy makers and education providers
   d. Reduce direct costs for SMEs: solving the money gap via programmes and funding

"It is important to recognize that intermediaries such as accountants can play an important role in upskilling SMEs. In particular, as they are in frequent contact with their businesses, they can create awareness on the topic and urge SME owners to take action in their best benefit."

Paul Gisby, Senior Manager Accountancy Europe

Stream 1. Strengthening ecosystems

Strengthening of the ecosystem revolves around the improvement of access for SMEs to knowledge, guidance and learning within their current and other ecosystems. As mentioned earlier, being connected and being embedded in regional or sectoral support structures - 'ecosystems' - is essential for SMEs' skills development. However, SMEs often lack access to such networks, to tacit and explicit knowledge and/or to facilities that help accelerate skills development. It can be difficult for them to organise shared services - which is easier in an ecosystem -, and the managerial capabilities to become anchored in ecosystems are sometimes lacking. Lastly, the availability of skills support structures throughout the EU is currently fragmented, with some regions having sufficient and adequate services in place, whereas in others no services were found at all when it comes to cybersecurity, big data and IoT skills.

"Digitalisation should not be seen as a goal in itself but as a means to achieve competitiveness: there must be a concrete need or a challenge to solve (saving time, better working processes etc.). Support services should thus never start with the technology itself but with the specific entrepreneurial problem to solve. The fore and foremost focus should be on the competitiveness of local firms."

Margarete Rudzki, Head of Unit Digital economy, SME policy, ZDH –German Confederation of skilled crafts and small businesses

Being connected and having access to knowledge, guides in the area of cybersecurity, big data and IoT, education and facilities is key for SMEs. As an interviewee put it: "for SMEs, it is either link or die. In every corner of Europe, SMEs need to be embedded in networks and have access to nearby support". In this respect, it is encouraging that the European Commission foresees a crucial role for the Digital Innovation Hubs (DIH) in providing SME support, with the goal of having one hub in every region by 2020[45]. DIHs are one-stop-shops where companies can access and test digital innovations, gain the required digital skills, get advice on financing support and ultimately accomplish their digital transformation. As stated by the EC Commissioner on Digital Economy and Society: "All companies should benefit of a DIH in their region to support the digital transformation. By ensuring a strong pan-EU network of DIHs with an investment of €100 min per year btw 2016-2020 we make sure everyone is included, in all regions"[46].

The measures for strengthening of the ecosystem (and initiatives) are clustered along three sub-goals:

A1 - Mapping of ecosystems

The mapping of ecosystems is aimed at determining the current state of play by mapping of existing ecosystems, identifying their strengths & weakness and increase transparency thereof. The overall aim of this sub-goal is to contribute to the availability of and access to regional support structures and facilitate the access of SMEs to concrete guidance, education and training in the area of cybersecurity, big data and IoT skills development offered by these regional support structures.

In order to gather the necessary intelligence on the ecosystems to meet these sub-goals, two measures are proposed. The first measure is the investment in research to understand the state of play & existing capacities. This includes, for example, the mapping of access points/hubs to improve transparency, undertake gap analysis, and the take-up of shared services centres.

The second measure is the creation of shared databases and tools to make information accessible to stakeholders. This allows more efficient distribution of information and insights, most notably best practices, among stakeholders.

A2 - Strengthening and expanding existing ecosystems

The strengthening and expansion of the existing ecosystems aims to support existing networks, hubs and initiatives to reach a more comprehensive coverage which will allow them access to every SME.

Three measures are proposed to achieve these aims. Firstly, policies and funding programmes that help to support SME communities, networks and ecosystems should be develop and supported. This measure is geared towards providing every SME in EU with a nearby hub where they can benefit from information, training, guidance on skills development. In particular, support to the Digital Innovation Hubs should be prioritised as good example of a hub that has enabled SMEs communities. Secondly, research on the existing policies and initiatives landscape is required to identify and promote good practices. This allows to leverage lessons learned from successful initiatives instead of reinventing the wheel. As part of this measure, clarifying the business case for SMEs may be an important step to make SMEs understand the importance of investment in cybersecurity, big data and IoT skills.

Thirdly, policies which help to mobilise accelerators/downstream actors need to be extended and, where no specific policies are in place yet, developed. In this measure, special attention needs to me given to ensure involvement of SMEs themselves to make sure policies are aligned with SME needs.

A3 - Boosting the effectiveness of the ecosystems

The boosting of the effectiveness of the ecosystems is aimed at ensuring that the support offered by the ecosystem to SMEs is optimally focused on achieving the overarching goal of e-skills development within SMEs. To this aim, two measures are proposed.

Firstly, EU and national programs that facilitate knowledge sharing should be initiated. Knowledge sharing allows stakeholder within the ecosystem to learn from others about the optimal method to support SMEs in their understanding of the need of investment in cybersecurity, big data and IoT skills and the ways in which to obtain these skills.

Secondly, a collaboration between hubs and education is expected to improve the match between demand for information and skills from the side of SMEs and its supply as offered by education. A better match ensures a more effective adaption of cybersecurity, big data and IoT by SMEs. One such example is the JADS MKB Data-lab in the Netherlands, which offers tools and solutions to SMEs that allow them to integrate data science into their business by means of PoCs.

Stream 2. Strategic outlook development

The technological savviness of SME owner/managers depends on a multitude of factors. Overall, SME owner/managers have difficulties understanding the impact of cybersecurity, big data and IoT technologies, or realising the urgency to act on it. A long-term vision on adopting cybersecurity, big data and IoT is lacking, and the focus is rather on operational matters. In addition to this internal perspective, also the technological maturity of the environment plays a role, as an environment stimulating for instance open data fosters the uptake of big data. To address this relative low 'tech maturity' of SMEs, the following actions are proposed to increase awareness and help them to design a strategy to adopt cybersecurity, big data and IoT technologies in their business models.

Bearing these developments in mind, the following sub-goals can further facilitate the access of SMEs to concrete guidance, education and training in the area of cybersecurity, big data and IoT skills development.

B1 - Raise awareness within SMEs

Instead of jumping into developing cybersecurity, big data and IoT skills, SMEs first need to be able to articulate their skills need: what are exactly the roles needed, and which skills do these roles need to have to work with cybersecurity, big data and IoT technologies? Information of SME managers and/or owners on the potential of the cybersecurity, big data and IoT technologies is an important first measure.

Specialised HR departments are often lacking in SMEs and a slow adoption of existing competence frameworks in existing trainings further contribute to a lack of awareness and difficulties in pinpointing the skills to be developed to benefit from cybersecurity, big data and IoT technologies. To address this challenge, the ecosystem of the SMEs can play a supportive role in raising awareness among SMEs by offering information.

Intermediaries can also play an important role in the adaption of cybersecurity, big data and IoT technologies within SMEs. Furthermore, if SME owner/managers do not know what they need, they are not able to assess whether it is more beneficial to internalise certain skills or to hire them on the market.

Intermediaries like accountants have a trusted relationship with SMEs, meaning they can also act as trusted advisor in relation to cybersecurity, big data and IoT adoption. Similarly, other stakeholders in the ecosystem may play a similar role in advising SMEs on cybersecurity, big data and IoT. Insurance companies are in frequent contact with SMEs and have a similar interest as the SMEs to prevent SMEs being exposed to societal risks (e.g. cyberattacks targeting the SME).

An alternative and more pressing route to raise awareness consists of legal obligation. Most notably, cybersecurity is an area with potential negative externalities in the form of network infection throughout a broader ecosystem. Consequently, there may be ground to consider legislation related to cybersecurity.

"As an insurance company, we want to contribute to a solid, safe and future-proof society. Cyber security for SMEs is becoming increasingly important and we have set up various activities to proactively inform SMEs about risks and mitigating measures. We have experienced that we are in a good position to raise the awareness of SMEs and support them in taking the right measures."

Danny Jaspers, Business lead Cybersecurity Achmea

B2 - Strengthen the direct business environment of SMEs

The technological savviness of SME owner/managers depends on a multitude of factors, of which one is age. Overall, SME owner/managers have difficulties understanding the impact cybersecurity, big data and IoT technologies, or realising the urgency to act on it. A long-term vision on adopting cybersecurity, big data and IoT is lacking, and the focus is rather on operational matters. In addition to this internal perspective, also the technological maturity of the environment plays a role, as an environment stimulating for instance open data fosters the uptake of big data. To address the above portrayed relatively low 'tech maturity', both internal and external, several measures are proposed.

First, collaboration with researchers can be stimulated to improve SMEs possibilities in the field of cybersecurity, big data and IoT. Second, continues investment in infrastructure will remain important as necessary condition to allow SMEs to build up a business case on investment in cybersecurity, big data and IoT. Third, a matchmaking platform can catalyse SMEs in their steps into cybersecurity, big data and IoT. As fourth and final measure, national cybersecurity frameworks can strengthen SMEs' business environment.

B3 - Facilitate collective action

One common challenge for SMEs is overcoming the small scale of the company, resulting in diseconomies of scale. Investment that are partly fixed, that is similar for each company, weight relatively heavier on small firms in comparison to large firms. To overcome this challenge, collective actions with other SMEs or with partners within the value chain may be used.

Most notably, SMEs may want to explore joint procurement and shared services. By sharing the burden among more parties, the (financial) barriers for SMEs reduce. One such example is the Cyber Resilience Center Brainport initiative in the Netherlands.[47]

Stream 3. Structured skills development

The technological savviness of SME owner/ managers depends on a multitude of factors, of which one is age. Overall, SME owner/ managers have difficulties understanding the impact of cybersecurity, big data and IoT technologies, or realising the urgency to act on it. A long-term vision on adopting cybersecurity, big data and IoT is lacking, and the focus is rather on operational matters. In addition to this internal perspective, also the technological maturity of the environment plays a role, as an environment stimulating for instance open data fosters the uptake of big data. To address the above portrayed relatively low 'tech maturity', both internal and external, the following sub-goals are identified.

C1 - Support implementation of structured skills development

Professionals possessing the specialised skills needed to work with cybersecurity, big data and IoT technologies are scarce. SMEs face several challenges in this regard, within the context of an ageing European workforce. SMEs compete with big corporates to attract and retain talents that possess the required combination of skills. And it is not just about attracting and retaining talents; also, continuous development of skills and knowledge is essential for the growth of their company. To overcome these challenges, this initiative foresees the following measures.

Existing initiatives form an important starting point. Plenty of blueprints, framework and tools are available that can support in their structured skills development. Examples in Europe include the e-Competence framework (e-CF) and the EDISON program for data science. In the United States, the NIST cybersecurity framework, can serve as an example. Key insights from the various blueprints, frameworks and tool may be bundled into a single, easily accessible starters guide for SMEs.

Also within value chains, various examples of actions supportive to SMEs skills development, most notably in cyber resilience, are available. One such example is the cyber resilience centre Brainport in the Netherlands.[48] In this initiative, the larger firms support SMEs with respect to their cybersecurity to improve the overall resilience of the entire value chain.

Structured skills development is bound to be more successful if a proper stocktaking of the skills potential within the company is properly assessed, for example by means of an aptitude test. One such a successful example is Skillnet Ireland, where a significant untapped potential for cyber skills turned out to be present.

"We need to act now and make SMEs more cyber secure. One of the most consistent needs of SME companies across all sectors and of all sizes is how to adequately protect their business in the face of the escalating cyber threat. Central to this need is the growing shortage of skilled cybersecurity personnel to protect against and respond to security breaches. By utilising Capture the Flag events, competence assessment tests and cyber webinars, we are educating SMEs in a way that can be replicated across the EU."

Dave Feenan, Network Manager at Technology Ireland ICT Skillnet

To make attraction of qualified external staff easier, a recognition mechanism for cybersecurity, big data and IoT skills. An important initiative to recognise informal learning is presented by the BDVA Skills Task Force[49].

C2 - Enhance capabilities for monitoring & decision-making in SMEs

Monitoring will support SMEs in understanding and strengthening their process of skills development. It will also allow to better assess where further strengthening is most needed and decide to invest.

One important measure for monitoring is the facilitation to self-assessment. To ensure any investment into skills training is effective, quality of trainings should be clear. For this purpose, quality labels for cybersecurity, big data and IoT trainings should be considered. Examples can be found is, inter alia, Germany[50] and the Netherlands[51]

Further enhancement of monitoring can be achieved in the form of stocktaking of market trends. As example, the market insights reporting initiative of VOICE, an association for IT-using SMEs, can be mentioned.[52]

"We want that all companies - big and small - can participate in the digital economy of tomorrow. For this aim, good digital skills, accessible to all, are indispensable!"

Arnaldo Abruzzini, CEO of Eurochambres

C3 - Increase transparency and access to funding

As for all investments, financing plays an important role. It is important to promote and scale successful funding mechanisms that foster skills development as well as to increase funding for skills development in SMEs.

Stream 4. Tailoring training to SMEs needs

Currently, too often available trainings in the area of cybersecurity, big data and IoT skills are not in line with SMEs' needs. Specific trainings in the area of cybersecurity, big data and IoT are scarce (focus is often on digital skills in the broadest sense), the form in which trainings are provided are not ideal for SMEs and too often, trainings are too expensive. Another problem is that the trainings that exist are not part of widely accepted framework. This results in difficulties with assessing the value of trainings. To address the current mismatch between available training offerings and SME's needs, the following measures contribute to ensuring a better match between available training offerings and training needs of SMEs.

Embarking on cybersecurity, big data and IoT technologies requires investments in several elements, of which one is training of personnel. Having restrained financial resources, SMEs need to prioritise their investments. An indirect return on investment may lead to the fact that training of personnel in the area of cybersecurity, big data and IoT is not among the top priorities. External funding is required but is not always available or is not easily accessible by SMEs.

The technological savviness of SME owner/managers depends on a multitude of factors, of which one is age. Overall, SME owner/managers have difficulties understanding the impact of cybersecurity, big data and IoT technologies, or realising the urgency to act on it. A long-term vision on cybersecurity, big data and IoT is lacking, and the focus is rather on operational matters. In addition to this internal perspective, also the technological maturity of the environment plays a role, as an environment stimulating for instance open data fosters the uptake of big data.

Professionals possessing the specialised skills needed to work with cybersecurity, big data and IoT technologies are scarce. SMEs face several challenges in this regard, within the context of an ageing European workforce. SMEs compete with big corporates to attract and retain talents that possess the required combination of skills. And it is not just about attracting and retaining talents: also for SME owner/managers, continuous development of skills and knowledge is essential for the growth of their company.

Training offerings should be set up so that they are tailored to the needs of SMEs and go beyond 'generic' digital skills, and rather focus specifically on cybersecurity, big data and IoT:

- Modular, blended, not necessarily during business hours. Innovative methods (eg gaming) should be explored.
- Focus specifically on cybersecurity, big data and IoT
- Trainings are practical, include whole chain, and include concrete examples
- Trainings are provided in a plain language and in the mother language of the SME

Easy participation by SME should be the leading guiding principle when developing the trainings. Both owners as well as skills specialists should be targeted with the trainings

"Demographic trends further impact shortages on the labour market. Collaboration between higher education and industry strengthens the ability to innovate and grow, and to increase the supply of digitally skilled employees in line with market needs. Innovations, such as online learning, and mobility of scarce expertise is key to support growth of the digital economy."

Timo Kos, Director Education and Student Affairs, Technical University Delft, and Director of Innovation, LDE Centre for Education and Learning

The following sub-goals enable the tailoring of training needs.

D1 - Increase education and training offers

Trainings are essential for skills development. For trainings to be optimally effective, they need to be closely aligned with the training needs. Further improvement of the understanding of training needs by education providers can support this alignment.

Although seemingly contradictory to the previous measure, trainings should make use of certain key principles to ensure optimal knowledge transfer.

The development of cybersecurity, big data and IoT skills throughout the company may go beyond just targeting the specialists (see the description of the previous measure). Especially inclusion of cybersecurity, big data and IoT modules in non-technical curricula will help to ensure broad support and understanding for the usefulness of cybersecurity, big data and IoT skills throughout the entire organisation.

Existing frameworks and blueprints can offer a solid and efficient basis for the further development of education and training offers. One example of such a source is DG Connect's Makes-me-digital initiative.[53]

To stimulate the attractiveness of cybersecurity, big data and IoT skills within education, enough internships should be ensured.

D2 - Develop training capacity

Currently, too often available trainings in the area of cybersecurity, big data and IoT skills are not in line with SMEs' needs. Specific trainings in the area OF cybersecurity, big data and IoT are scarce (focus is often on digital skills in the broadest sense), the form in which trainings are provided are not ideal for SMEs and too often, trainings are too expensive. Another problem is that the trainings that exist are not part of widely accepted framework. This results in difficulties with assessing the value of trainings. To address the current mismatch between available training offerings and SME's needs, the following measures contribute to ensuring a better match between available training offerings and training needs of SMEs.

Increase in mobility of scarce experts was achieved in Sweden[54]. For an effective out-roll of training, sufficient training facilities suitable should be available[55].

D3 - Collect intelligence

Training development may be supported by data on SME trainings needs and participation motives. Achieve better insight into SME training needs to align policy and training offers by collecting SME consumption levels of trainings. Aggregation of data, either at regional level and/or national level, may provide insightful patterns to identify SME needs.

D4 - Reduce direct costs for SMEs

Embarking on cybersecurity, big data and IoT technologies requires investments in several elements, of which one is training of personnel. Having restrained financial resources, SMEs need to prioritise their investments. An indirect return on investment may lead to the fact that training of personnel in the area of cybersecurity, big data and IoT is not among the top priorities. Funding has been discussed in stream C3. Here, the focus lies on reduction of the direct costs. The following measures can be considered.

Innovation voucher scheme have proven their worth in, inter alia, Finland, the Netherlands and Lithuania.[56]

Delivering the roadmap: Ecosystems are crucial for empowering SMEs

Governance: Creating overarching governance for skills

There is a need to create a stronger partnership between the public and the private sector in order to offer leadership and vision for digital skills and jobs in Europe. This entails a specific commitment from all the stakeholders in order to pursue common objectives and make investments to achieve them.

Build and further develop public-private partnerships on ICT skills and jobs, including industry and trade associations, national, regional and local governments, companies, education institutions, research and ICT professionals. Our recommendation is for the **establishment a European Public Private Partnership (PPP)** for Skills and Jobs, as such entity is perfectly suited to enable a **long-term, strategic approach** and reduce uncertainties by allowing for long-term commitments.

In addition, this PPP needs to be accompanied by close collaboration with research and universities as well as industry to develop an evidence-based approach to skills development, that can help identify future skills needs for the digital transformation.

This strategic and evidence-based approach to skills development needs to consider market needs, thus laying the basis for innovation in Europe. It is important differentiate between the different types of new technologies or skills. For instance, cybersecurity is a horizontal topic, but big data or IoT depend very much on the specific business model of a company. Thus, there is a need to distinguish measures according to market demands and needs, and therefore, to base action on evidence and research on market demands.

"We need to make cybersecurity knowledge easy and intuitive accessible for SMEs via a platform. It should contain concrete guidance and examples of how to make the company more secure, targeting also those employees that already have some digital skills such as the IT-administrator who could then be enabled to implement the quick fixes."

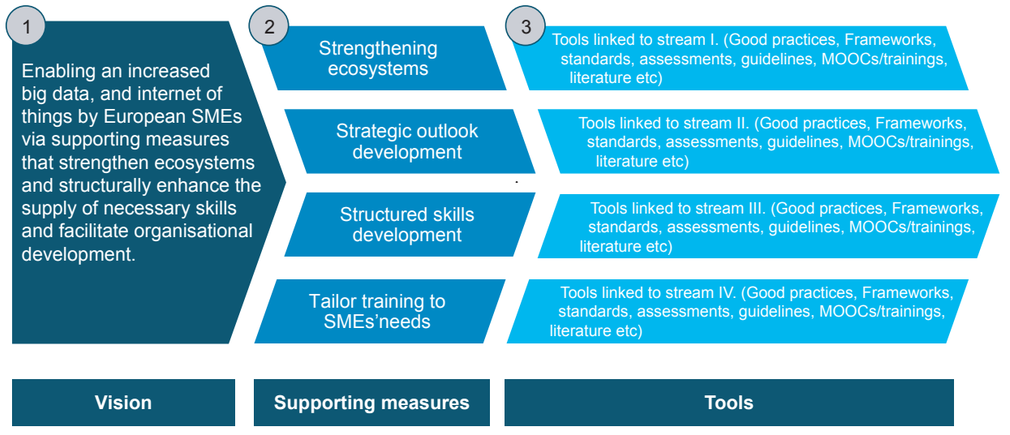
Gorden Kirstein, CEO Movetech (a German cybersecurity SME)

A practical toolbox supporting implementation of the roadmap

The purpose of the toolbox is to facilitate knowledge sharing and to encourage stakeholders to engage in (new) initiatives that will support SMEs in adopting new technologies and developing the required skills. It aims to point stakeholders towards tools that have demonstrated a certain added value and that can help others in setting-up or scaling up initiatives.

In this approach, the tools are mapped to the streams in the roadmap. This should allow for an intuitive understanding of 'what' to find 'where'. As an example, assuming a stakeholder is planning to develop an initiative aimed at supporting SMEs with structured skills development (stream 3), he/she will find relevant materials mapped to that stream.

Figure 8 Meta-model of the toolbox



"Emilia-Romagna is increasingly an international platform for innovation and big data and supercomputing. We support knowledge, skills, infrastructures for a new stable employment and enhancement of the territories of Southern and Mediterranean Europe in particular. Knowledge sharing and strengthening ecosystems - from our region to the European level - is essential to grow."

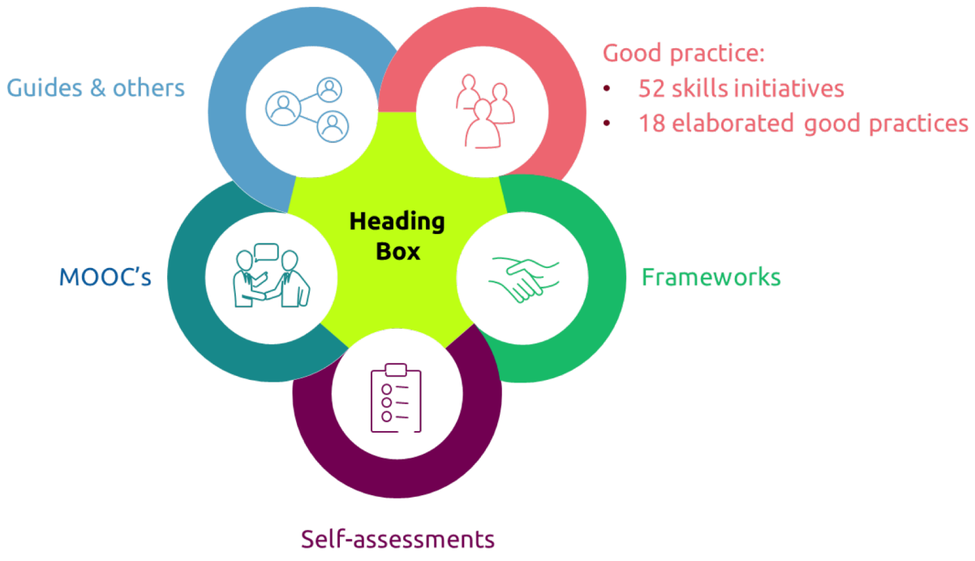
Morena Diazzi, Director-General of the Emilia-Romagna Regional Government for Knowledge, Labour and Enterprise Economy

The following initiatives were selected as good practices

- Skillnet Ireland by the government of Ireland
- Cybersecurity Skills Initiative (CSI) by an Irish nationwide public-private coalition
- SME Datalab by Jheronimus Academy of Data Science (JADS)
- PROMPT by RISE Research Institutes of Sweden
- Cyber Resilience Centre by Brainport Eindhoven region
- ASTER by Emilia-Romagna region
- Recognising skills in data science by the Big Data Value Association (BDVA)
- Community knowledge platform by VOICE (association of IT-using SMEs)
- SMESEC by the SMESEC consortium for the European Commission
- Make_SME_Digital (Blueprint skills training SMEs LT an ES) by consortium for the European Commission
- Mittelstand 4.0 Centres of Excellence by the Federal Ministry for Economic Affairs and Energy Germany
- Les Digiteurs by CCI Paris Ile-de France
- SEnDIng by the University of Patras for the European Commission
- Modern Enterprises Programme by the Hungarian Chamber of Commerce
- Innovation vouchers by Business Finland

Three International:

- Cybersecurity support rangers by The Ministry of Economy, Trade and Industry Japan
- Cyber NYC by the New York City
- Skillsfuture initiative by Singapore government



Footnotes

1. The project developed four streams to support the vision of enhancing SME skills in IoT, Big Data and Cybersecurity: (I) Strengthening ecosystems, (II) Strategic outlook development, (III) Structured skills
2. The ecosystem (consisting of clusters, associations or chambers and the supply chain and business environment of SMEs) needs to be aware of skills needs: - they are the intermediaries that can raise awareness among SMEs or develop collective action to bridge a skills gap, e.g. by offering VET training in collaboration with SMEs or by establishing stronger partnerships with universities or research communities, or by designing training programmes according to SMEs' needs. At the same time, they need to work towards developing the capacity for strategic outlook in SMEs. SMEs need to be aware of their skills needs and develop strategies to fulfil them. These insights and actual training schemes need to be developed at the local level - the EU level will only be responsible for the sharing of best practices and developing "blueprints" based on successful cases.
3. See ICT Competence Center initiative in Berlin
4. European Commission (2017), State of the Union 2017 - Cybersecurity: Commission scales up EU's response to cyber-attacks. Published September. Available at: http://europa.eu/rapid/press-release_IP-17-3193_en.htm
5. Cyber Ventures (2017), 2017 Cybercrime report. Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
6. Hamilton Places Strategies (2016), Cybercrime costs more than you think. Published February. Available at: https://www.hamiltonplacestrategies.com/insights/cybercrime-costs-more-you-think/
7. The Guardian (2016), Huge rise in hack attacks as criminals target small businesses. Available at: https://www.theguardian.com/small-business-network/2016/feb/08/huge-rise-hack-attacks-cyber-criminals-target-small-businesses
8. IQ in IT (2017), Why cybersecurity for SMEs is even more important in 2017. Available at: https://www.iqin.it/blog/why-cyber-security-smes-even-more-important-2017
9. The Guardian (2018), UK businesses face growing threat from cyber-attacks - report. Published April. Available at: https://www.theguardian.com/technology/2018/apr/10/uk-businesses-face-growing-threat-from-cyber-attacks-report
10. Mazzarol, T. (2015), SMEs engagement with e-commerce, e-business and e-marketing, Small Enterprise Research, 22:1, 79-90. https://doi.org/10.1080/13215906.2015.1018400 & Enisa (2016), Information security and privacy standards for SMEs. Published June. Available at: https://www.enisa.europa.eu/publications/standardisation-for-smes
11. Ibid.
12. Fresh Business Thinking (2016), Cybersecurity is a growing priority – don't be the weak link. Published May. Available at: http://www.freshbusinessthinking.com/cybersecurity-is-a-growing-priority-dont-be-the-weak-link/
13. SMESEC (n.d.), A lightweight cybersecurity framework for thorough protection. Available at: https://smesec.eu/index.html
14. Cybersec (2017), European cybersecurity market. Published June. Available at: https://cybersecforum.eu/en/the-2nd-issue-of-the-european-cybersecurity-market-already-available-download/
15. Cyber Ventures (2017), 2017 Cybercrime report. Available at: https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf
16. MicroMarketMonitor (n.d.), Europe cybersecurity market. Available at: http://www.micromarketmonitor.com/market/europe-cyber-security-4129808188.html
17. https://ec.europa.eu/digital-single-market/en/news/state-union-2018-cybersecurity-commission-proposes-invest-stronger-and-pioneering-cybersecurity
18. European Commission (2017), Enter the data economy: EU policies for a thriving data ecosystem. Published January. Available at: https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_21.pdf
19. European Commission (2017), Building a European data economy. Published January. Available at: https://ec.europa.eu/digital-single-market/en/policies/building-european-data-economy
20. IDC (2017), European Data Market Study Final Report SMART 2013/0063. Report prepared for the European Commission. Available at: https://www.key4biz.it/wp-content/uploads/2018/04/SMART20130063_Final-Report_030417_2.pdf
21. Ibid.
22. Spencer, L. (2014), Internet of Things market to hit $7.1 trillion by 2020: IDC. Published June. Available at: http://www.zdnet.com/article/internet-of-things-market-to-hit-7-1-trillion-by-2020-idc/
23. Macaulay, J., Buckalew, L., & Chung, G. (2015), Internet of Things in logistics. Available at: http://www.dhl.com/content/dam/Local_Images/g0/New_aboutus/innovation/DHLTrendReport_Internet_of_things.pdf
24. IDC & TXT (2015), Definition of a research and innovation policy leveraging cloud computing and IoT combination. Report prepared for the European Commission. Available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
25. European Commission (2016), Advancing the Internet of Things in Europe. Published April. Available at: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A52016SC0110
26. IDC & TXT (2015), Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Report prepared for the European Commission. Available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
27. Among others: Information Age (2017), US and Europe businesses lag behind in IoT adoption. Published February. Available at: http://www.information-age.com/us-europe-businesses-lag-behind-iot-adoption-123464372/ & Capgemini (2018), Unlocking the business value of IoT in operations. Available at: https://www.capgemini.com/wp-content/uploads/2018/03/dti-research_iot_web.pdf
28. European Commission (2014), Definition of a Research and Innovation Policy Leveraging Cloud Computing and IoT Combination. Available at: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=9472
29. Ibid.
30. Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorelle, X. & M. Seabra Reis (2016), How Can SMEs Benefit from Big Data? Challenges and a Path Forward. Quality and Reliability Engineering International, Special Issue Article. https://doi.org/10.1002/qre.2008
31. Coleman, S., Göb, R., Manco, G., Pievatolo, A., Tort-Martorelle, X. & M. Seabra Reis (2016), How Can SMEs Benefit from Big Data? Challenges and a Path Forward. Quality and Reliability Engineering International, Special Issue Article. https://doi.org/10.1002/qre.2008
32. IDC (2017), European Data Market Study Final Report SMART 2013/0063. Report prepared for the European Commission. Available at: http://datalandscape.eu/
33. E-Skills UK (2013), Big Data Analytics Adoption and Employment Trends, 2012-2017. Available at: https://www.thetechpartnership.com/globalassets/pdfs/research-2013/bigdataanalytics_report_nov2013.pdf
34. Vossen G, Lechtenbörger J, Fekete D. (2015), Big data in kleinen und mittleren Unternehmen - eine empirische Bestandsaufnahme. Westfälische Wilhelms-Universität Münster, Germany. Available at: http://www.wi1.uni-muenster.de/pi/iai/publikationen/BigData.pdf
35. Capgemini (2018), Unlocking the business value of IoT in operations. Available at: https://www.capgemini.com/wp-content/uploads/2018/03/dti-research_iot_web.pdf
36. Ibid.
37. European Commission (2015), Definition of a research and innovation policy leveraging cloud computing and IoT combination. Published May. Available at: https://ec.europa.eu/digital-single-market/en/news/definition-research-and-innovation-policy-leveraging-cloud-computing-and-iot-combination
38. Ericsson, Deloitte & DI Digital (2015), Every. Thing. Connected. A study of the adoption of 'Internet of Things' among Danish companies. Published July. Available at: https://digital.di.dk/SiteCollectionDocuments/Analyser/IoT_Report_onlineversion.pdf
39. The Economist (2017), The Internet of Things business index 2017. Available at: https://www.eiuperspectives.economist.com/sites/default/files/EIU-ARM-IBM%20IoT%20Business%20Index%202017%20copy.pdf
40. Cagemini (2017), Cybersecurity talent: The big gap in cyber protection. Available at: https://www.capgemini.com/wp-content/uploads/2018/02/the-cybersecurity-talent-gap-v8_web.pdf
41. ENISA (2015), Information security and privacy standards for SMEs. Recommendations to improve the adoption of information security and privacy standards in small and medium enterprises. Available at: https://www.enisa.europa.eu/publications/standardisation-for-smes/at_download/fullReport
42. Ibid.
43. Berghaus, S. & Beck, A. (2016), Stages in digital business transformation: results of an empirical maturity study. Available at: https://pdfs.semanticscholar.org/d416/aa50e0eb6abb3f5e6e5fa071931f9a494d28.pdf
44. The vision was developed and validated during three expert workshops, a steering committee meeting, 50 in-depth interviews and an online survey held between January 2018 and February 2019, with approximately 150 experts representing different backgrounds participating.
45. https://ec.europa.eu/digital-single-market/en/blog/digital-innovation-hubs-joining-forces-accelerate-digital-transformation-european-industry
46. https://twitter.com/GabrielMariya/status/1027330339734253569
47. https://www.brainport.nl/nieuws-ontwikkelingen/primeur-brainport-eindhoven-voor-ketenweerbaarheid-cybersecurity
48. https://cwbrainport.nl
49. https://www.digitalsme.eu/digital/uploads/20190412_4th-Workshop_2nd-ppt_Presentation-BDVe.pdf
50. Trusted Cloud Initiative (https://www.trusted-cloud.de/).
51. https://mkb.nl/nieuws/bedrijfsleven-ontwikkelt-risicomodel-en-keurmerk-cyberbeveiliging
52. https://voice-ev.org/wissensplattform/
53. https://makesmedigital.eu
54. Malin Rosqvist, Driving innovation and improving competences in Swedish SMEs; https://www.digitalsme.eu/digital/uploads/3rd-Workshop_1st-ppt_2019-02-08_MalinRosqvist.pdf
55. See, for example, Recommendation from thesis IoT matchmaking platform for SMEs (TU Delft); https://repository.tudelft.nl/islandora/object/uuid:e31a8e50-8f7c-4601-ad97-27a292092554/datastream/OBJ
56. https://www.businessfinland.fi/en/for-finnish-customers/services/funding/sme/innovation-voucher/; https://www.verslilietuva.lt/paslaugos/kompetenciu-vauceris/

European Commission

Supporting specialised skills development: Big Data, Internet of Things and Cybersecurity for SMEs
EASME/COSME/2017/007

Luxembourg, Publications Office of the European Union, 2020

48 pages.

ISBN: 978-92-9202-779-7
doi: 10.2826/708138

EA-01-20-013-EN-N

Publications Office
of the European Union

ISBN: 978-92-9202-779-7
DOI: 10.2826/708138