PARP
PFR Group

Branżowy Bilans
Kapitału Ludzkiego II

Sectoral Human Capital Study II

Telecommunications and Cybersecurity

Chosen results from the 2nd edition of the study

European Funds
Knowledge Education Development

Republic of Poland

European Union
European Social Fund

About the study

Project name

Sectoral Human Capital Study II
Telecommunications and Cybersecurity
(2nd edition)

Study objective

To increase awareness of current and future demand for competencies in the Telecommunications and Cybersecurity sector

Schedule

June 2022 to June 2023

Definition of the sector (based on NACE)

Wired telecommunications activities (NACE J.61.1)
Wireless telecommunications activities (NACE J.61.2)
Satellite telecommunications activities (NACE J.61.3)
Other telecommunications activities (NACE J.61.9)
Cybersecurity (under NACE J.62.03 – Computer facilities management activities)

Methodology

Qualitative research

(fieldwork: July 2022 to November 2022)

20 individual interviews with employers

4 expert panels

Delphi survey with 43 industry experts

Summary panel with the Sectoral Competence Council, Telecommunications and Cybersecurity

Quantitative research

(fieldwork: February 2023 to March 2023)

Surveys with employers from the industry (n = 803) and employees employed in key positions for the industry (n = 1011)

Factors with an impact on the sector

External factors:

inflation

energy crisis

COVID-19 pandemic

the war in Ukraine

interrupted or limited supply chains

Internal* factors:

- outflow of highly qualified specialists to foreign companies [T][C]
- development of wireless connectivity (5G networks) and fibre-optic infrastructure [T]
- providing employees with opportunities for personal development [C]
- growing demand for cybersecurity services [C]

* sectors affected by factor: C – Cybersecurity; T – Telecommunications

Source: own study based on the results of the quantitative survey of employers (n = 803) and qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Challenges* in the Telecommunications and Cybersecurity sector

Safety Assurance

- **53%** recognise the need to develop security measures and identify vulnerabilities for new solutions/technologies [C]

Personnel problems

- **52%** recognise the difficulty in retaining specialists before moving to foreign companies [C: 62%, T: 50%]
- **47%** draw attention to the problem of finding new employees in the IT industry [C: 55% ,T: 46%]
- **46%** of employers envisage problems finding specialists in cybersecurity [C: 52%, T: 45%]

Globalisation

- **39%** of employers see a need for increasing international competitiveness [C: 36%, T: 40%]

Care for the user

- **37%** employers see a need for increasing attention on the user experience [T]

* sectors affected by factor: C – Cybersecurity, T – Telecommunications

Source: own study based on the results of the quantitative survey of employers (n = 803) and qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Scenarios of the sector’s future

The research project led to the development of three scenarios of the sector’s future, showing action strategies that have the potential to be implemented in the future by companies in the industry, depending on the intensification or weakening of individual factors affecting the industry.

Scenario 1

Active internal company development

Possible implementation in case of enterprises offering proprietary services or having their own products that they want to develop.

Scenario 2

Implementation of activities through external contractors

Possible implementation in the case of enterprises providing services or projects in a specific sector or in several sectors for many clients.

Scenario 3

Active collaboration with scientific institutions

Possible implementation in the case of both companies offering their own services and/or products, and those providing services or projects for different companies

Source: own study based on the results of the qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Scenarios of the sector's future

Scenario 1
Active internal company development

Which companies might implement this strategy?

- Enterprises offering proprietary services or products they want to develop
- Enterprises of all sizes (although above all medium and large companies), financially stable, and with adequate resources to develop internal teams

Expected of companies implementing this strategy:

- they will try to cope with the shortage of specialists by creating their own internship programmes or bootcamps (training camps)
- to reduce employee turnover, they will invest in improving the level of employee competencies, mainly by organising internal and external company training and courses, as well as providing access to the most important industry events
- in the context of collaboration with the education sector, they will undertake and co-create initiatives such as organising space for discussion, exchanging proposals, and providing information about current demand for employees and individual competencies among employers
- they will attend to issues of corporate social responsibility and education of the public

Source: own study based on the results of the qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Scenario 2
Implementation of activities through external contractors

Which companies might implement this strategy?

- Enterprises providing services or projects in a specific industry or in several industries for multiple clients
- Micro and small companies that do not have (or do not want to spend) funds to build permanent, internal teams

Expected of companies implementing this strategy:

- they will switch from permanent employment (especially hiring based on employment contracts) in favour of contract workers
- they will not be particularly interested in attending to the development of employees' competencies due to the specificity of employing staff; businesses will expect workers to have all the necessary competencies enabling the proper implementation of a given project
- in the context of collaboration with the education sector, they will participate in various initiatives mainly to provide information on current demand for employees and competencies in the industry, but they will not get deeply involved
- they will invest in creating their own projects aimed at raising general public awareness of cybersecurity or threats related to new digital technologies

Source: own study based on the results of the qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Scenarios of the sector's future

Scenario 3
Active collaboration with scientific institutions

Which companies might implement this strategy?

- Both companies offering their own services or products, as well as those providing services or projects for different companies
- Mainly medium and large enterprises with adequate financial resources allocated for development, companies that are able to "freeze" for new employees, despite the delayed return on investing in them

Expected of companies implementing this strategy:

- in order to avoid the main problem, which is the shortage of industry specialists on the labour market, they will take steps aimed at establishing collaboration between education and business, with schools and universities educating in fields related to the industry (patronage classes, scholarship programmes)
- they will be focused on creating in-office or hybrid teams due to the desire to integrate employees recruited through internship programmes and patronage classes and the need to create an environment conducive to the transfer of knowledge to new employees by existing specialists

Source: own study based on the results of the qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

The sector and the future

Changes planned by companies within the next 3 years:

64% increase in the price of services

47% greater outlay on innovation in the company

42% new or increased investment in new technologies (machine learning, artificial intelligence) and modern software

39% launching new products/ services

38% new or increased investment in the development of employee skills

36% the automation of selected processes in the company

32% starting or intensifying R&D work in the company, either by itself or in collaboration with academic institutions

29% involvement or increased company involvement in collaboration with schools or universities in order to educate and acquire future workers

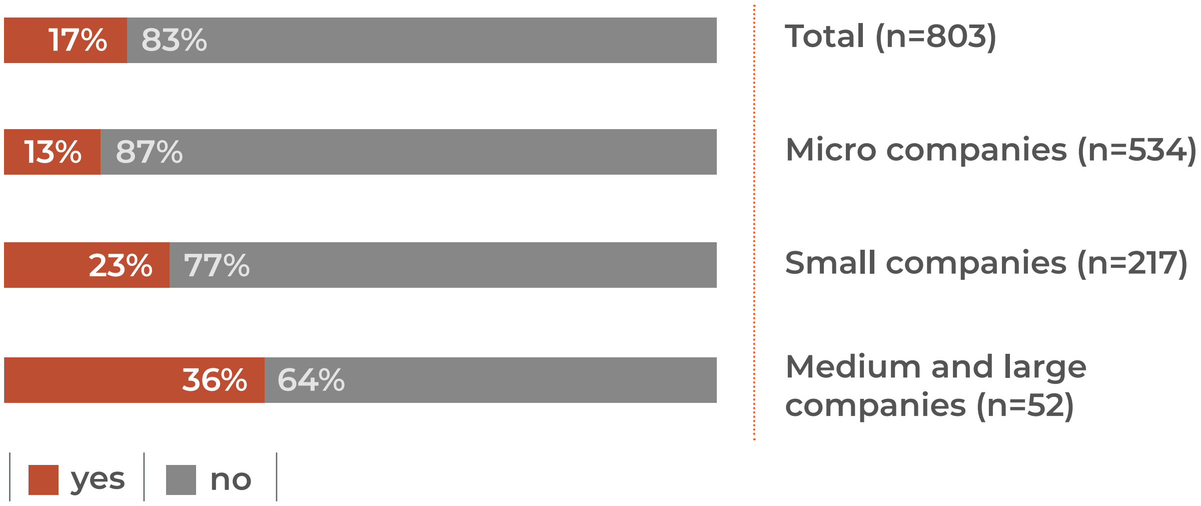
Source: own study based on the results of the quantitative survey of employers (n = 803) carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Demand for workers in the industry

In the 12 months preceding the survey, **17% of companies** in the industry **were looking for new workers**

The bigger the company, the higher the percentage looking for employees

Searching for employees for the company



The following were searched for **most frequently**:

Developer **22%**

Engineer (regardless of specialisation) **22%**

Systems architect **13%**

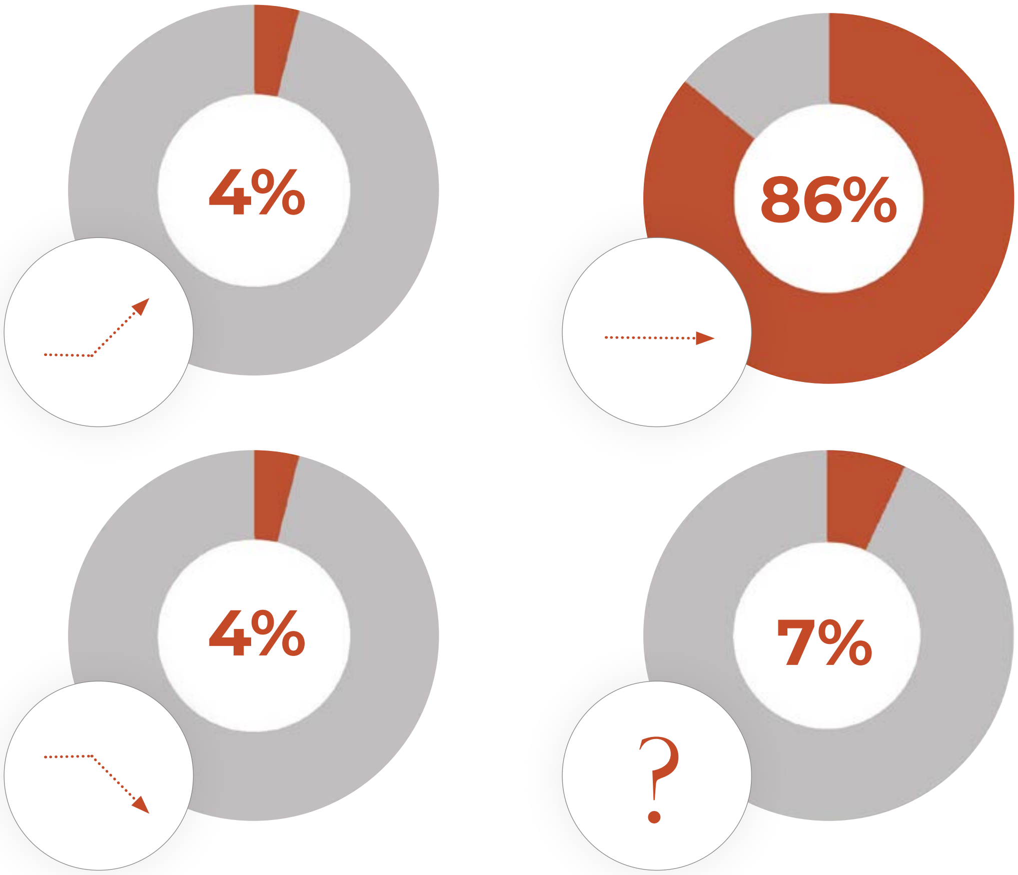
Commercial director **13%**

Project manager **10%**

Source: own study based on the results of the quantitative survey of employers (n = 803) carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Forecast changes in employment

Regardless of the sector, **more than 85% of companies** in the industry believe that its **level of employment will remain unchanged** in the 12 months after the survey



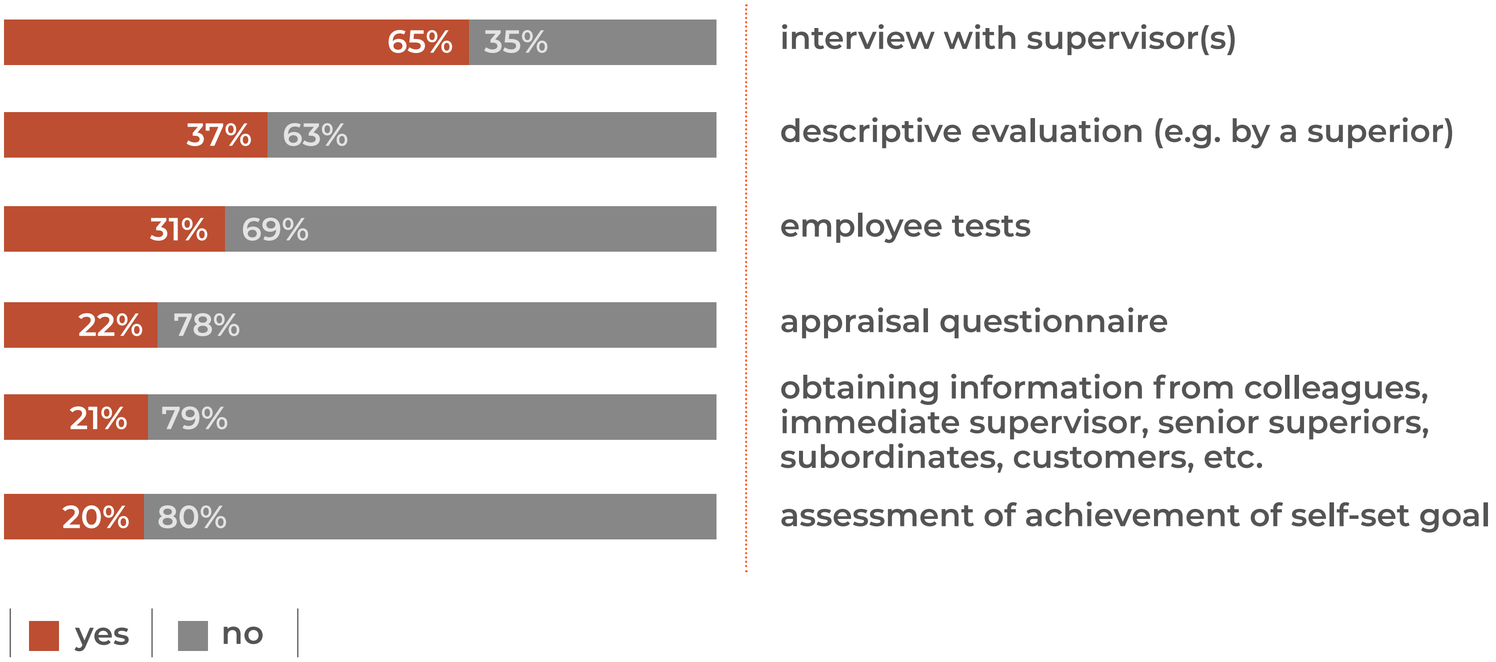
- **4%** increase
- **86%** no change
- **4%** decrease
- **7%** don't know/hard to say

Source: own study based on the results of the quantitative survey of employers (n = 803) carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Assessing employees' skills

56% of employees employed in key positions **are assessed** by employers **in terms of the skills** they need; **one in three** is being assessed systematically (at least once a year)

Ways of assessing employees' skills



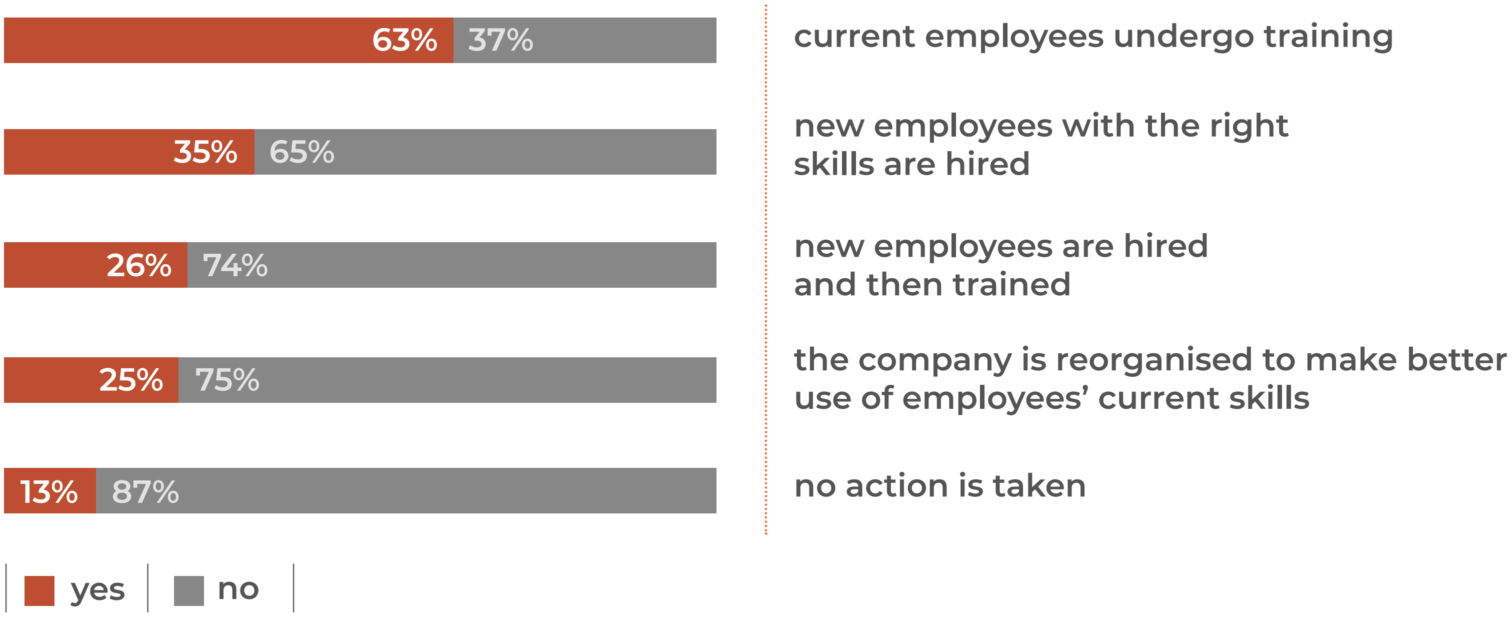
Source: own study based on the results of the quantitative survey of employees (n = 1011) carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Employers’ strategies for dealing with competence deficits

59% of employers rate the competencies of their employees as fully meeting their expectations

38% of employers see a need to improve their employees’ competencies

But what about when certain competencies are lacking?



Source: own study based on the results of the quantitative survey of employers (n = 803) carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Balance of competencies

Balance of competencies – a compilation of assessments of key competencies for specific positions in the telecommunications and cybersecurity sector from the perspective of employers and employees, in order to better balance the labour market in terms of the supply of workers with the right competencies and employers' demand for them.

In the quantitative survey, **employers** referred to competencies in terms of:

- the importance of the competence for the performance of professional duties,
- difficulty in finding a person who has a specific competence needed to work in a given position,
- projections of the change in importance of this competence over the next three years.

Employers' opinions served as the basis for distinguishing the so-called hot skills, i.e. skills whose importance is growing or will grow rapidly over the next 3 years.

On the other hand, **employees** in the quantitative survey assessed their own level of competencies assigned to their position, as well as their willingness to develop them.

Balance of competencies

- In terms of percentage, the largest share of hard-to-find competencies was recorded for the following positions: system architect and quality assurance in the telecommunications sector, and pen-tester and security expert in the cybersecurity sector*.

- Hot skills competencies – defined according to the adopted assumption – occur primarily in the cybersecurity sector*. For example when it comes to:
  - CISO, a hot skill is knowledge in the field of information security and computer technologies,
  - security architect, hot skills are knowledge of computer technology and the ability to predict how an attack on a system, program or service could occur,
  - pen-tester, a hot skill is knowledge in the field of information security (e.g. personal data, company data, data storage methods),
  - SOC coordinator, a hot skill is the ability to block threats.

* In the context of positions in the cybersecurity sector, due to the low sample sizes the results should be treated as illustrative.

Source: own study based on the results of the quantitative survey of employers (n = 803) carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

Competencies of the future

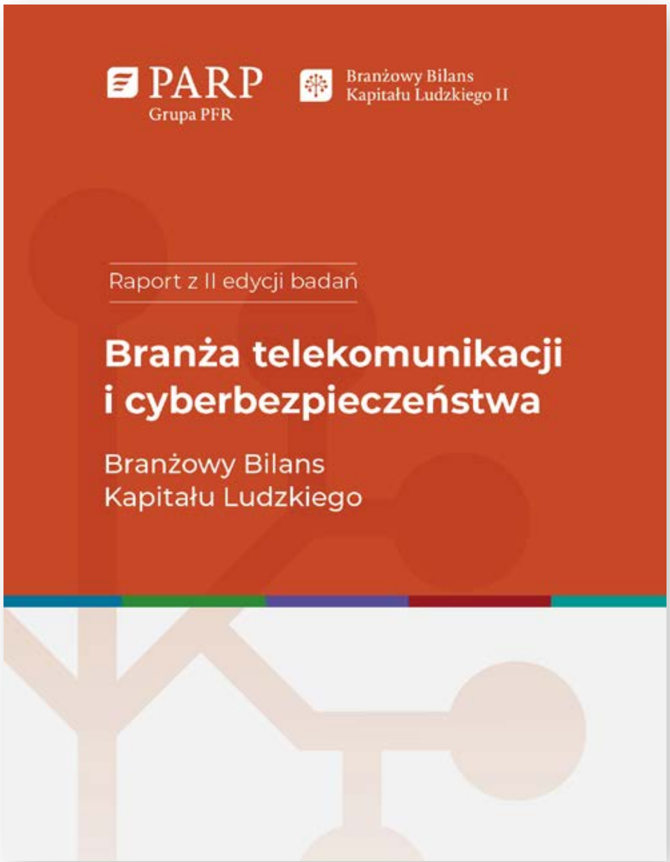
Competencies of the future, which – in the opinion of industry experts expressed in the qualitative research – will appear in the competence profile of a given position.

Key position	Competences of the future
IT Architekt	• knowledge in the field of artificial intelligence (AI), especially machine learning • creating systems based on new methods of implementation (microservices, cloud technologies)
Developer	• knowledge in the field of artificial intelligence (AI), especially machine learning • ability to use generative AI tools to write code
Quality assurance	• ability to write automated tests for software written in cloud systems or in microservices architecture
Engineer	• knowledge in the field of designing devices and sensors used in the Internet of Things (IoT) technology
Project manager	• ability to build teams in relation to the preferred work model (remote, on-site, mixed teams) and interdisciplinary teams
Security auditor	• knowledge of the latest certification standards (for example meeting relevant security standards using new digital technologies such as AI, IoT)
Penetration tester	• knowledge in the field of artificial intelligence (AI), especially machine learning • Internet of Things (IoT) knowledge
Chief Information Security Officer (CISO)	• securing physical and digital data against cyberattacks using new technologies (e.g. AI)
Security architect	• protection of analogue and digital data against cyberattacks using new technologies (e.g. AI)
Security Expert	• lack of indicated competencies
Security Operations Centre (SOC) Coordinator	• lack of indicated competencies
Sales manager	• lack of indicated competencies

Source: own study based on the results of the qualitative survey carried out as part of the BBKLII project in the telecommunications and cybersecurity industry, 2nd edition.

A full discussion of the research findings can be found in the report:

Sectoral Human Capital Study II – Telecommunications and Cybersecurity. Report on the 2nd edition of the study


PARP
Grupa PFR
Branżowy Bilans
Kapitału Ludzkiego II
Raport z II edycji badań

Branża telekomunikacji i cyberbezpieczeństwa

Branżowy Bilans
Kapitału Ludzkiego