University of Maribor

Faculty of Electrical Engineering and Computer Science

FERI

Developing cyber security training programmes – RUKIV

Marko Hölbl,

University of Maribor

Slovenian Research and Innovation Agency

Frequency of cyber security competences in educational programmes

Motivation

- Apart from Slovenia, Croatia, Luxembourg and Malta are the only other EU countries without their own higher education programme in cyber security
- CYBERHEAD (Cybersecurity Higher Education Database)
  - managed by ENISA (European Cyber Security Agency)
- The Slovene Research Agency funded a project to develop training (including a study programme) in cybersecurity

Developing cyber security training programmes – RUKIV

Aim

- Frequency of cyber security competences in educational programmes
  - Overview of the competences or skills taught in higher education study programmes in the field of cyber security.
  - The results will be:
    - demonstrate the importance of specific skills,
    - guide how to structure cybersecurity degree programmes; and
    - give guidance on what content to include in the curriculum.

- Useful for designing well-balanced study programmes and/or for analysing gaps in knowledge coverage.

Methodology

- Knowledge model
  - Cybersecurity Curricula 2017: Curriculum Guidelines for Post-Secondary Degree Programmes in Cybersecurity
    Jointly prepared by ACM, IEEE CS, AIS SIGSEC and IFIP WG 11.8.

- Random 12 study programmes included (9.5%)
  - From the CYBERHEAD repository (126 bachelor's and master's programmes)
  - Evaluate or classify content

Results

- Evaluation
  - Classification of the content of the 55 courses according to their descriptions
  - Scoring is proportional to the number of knowledge units covered by the course
  - Separate scoring normalised according to the work required to complete the course (ECTS points).

#	Points	Area of knowledge	Area of knowledge	ECTS points
1	51,37	Data security	Data security	247,97
2	29,45	Connection security	Connection security	144,14
3	24,35	Organisational security	Organisational security	115,72
4	23,00	Software security	Software security	109,39
5	18,89	Social security	Security of systems	97,21
6	18,58	Security of systems	Social security	91,85
7	14,70	Human security	Human security	72,48
8	3,67	Component security	Component security	17,23

Results

- Findings (knowledge units)
  - Cryptography and Network Defence are ranked in the top
- Lower-ranked knowledge units are typically addressed in less challenging subjects (i.e. subjects with fewer ECTS points).
  - In contrast, Secure Communication is the subject of more extensive courses

#	Points:	Knowledge units	Knowledge units	ECTS points
1	18,28	Cryptography	Cryptography	81,72
2	9,79	Network defence	Network defence	46,17
3	7,88	Integrity and authentication	Control of systems	44,58
4	7,41	Analysis and testing	Integrity and authentication	43,01
5	7,34	Monitoring of systems	Analysis and testing	34,85
6	6,56	Design	Cryptanalysis	34,58
7	6,40	Cryptanalysis	Design	33,02
8	5,16	Cyber law	Cyber law	24,91
9	4,97	Digital forensics	Risk management	23,37
10	4,86	Risk management	Cybercrime	22,90
11	4,65	Network architecture	Network architecture	22,46
12	4,50	cyber policy	Security management and policy	21,41
13	4,32	Cybercrime	cyber policy	21,37
14	4,07	Typical system architectures	Systems thinking	19,19
15	4,06	Access control	Access control	19,14
16	4,02	Systems thinking	Secure communication protocols	18,95
17	3,99	Security management and policy	Fundamental principles	18,80
18	3,94	Fundamental principles	Digital forensics	18,78
19	3,81	Network services	Network services	18,46
20	3,46	Information storage security	Cybersecurity planning	17,53
21	3,41	Cybersecurity planning	Data privacy	16,21
22	3,32	Cyber ethics	Awareness and understanding	16,13
23	3,31	Awareness and understanding	Information storage security	15,59
24	3,24	Secure communication protocols	Hardware architecture	15,13
25	3,07	Data privacy	Cyber ethics	14,90
26	3,03	Hardware architecture	Typical system architectures	14,34
27	2,86	Analytical tools	Distributed systems architecture	14,13
28	2,75	Useful security and privacy	Analytical tools	13,96
29	2,69	Business continuity, disaster recovery and incident management	Implementation	13,83
30	2,65	Distributed systems architecture	Useful security and privacy	12,42
31	2,65	Identity management	Identity management	12,34
32	2,52	Implementing networks	Implementing networks	12,21
33	2,51	Implementation	Business continuity, disaster recovery and incident management	11,84
34	2,39	Security operations	Social engineering	10,51
35	2,06	Physical interfaces and connectors	Physical interfaces and connectors	10,12
36	2,03	Systems management	Privacy and security of personal data	9,07
37	1,89	Privacy and security of personal data	Managing security programmes	8,93
38	1,79	Personal compliance with cybersecurity rules/policies/ethical norms	System access	8,81
39	1,62	Component design	Component design	8,06
40	1,59	Privacy	Systems management	7,93
41	1,47	Social engineering	Privacy	7,77
42	1,43	Managing security programmes	Personal compliance with cybersecurity rules/policies/ethical norms	7,76
43	1,43	System access	Security operations	7,71
44	1,22	Installation and maintenance	Systems management	7,08
45	1,17	Systems management	Physical media	5,46
46	1,17	Reverse engineering of components	Component testing	5,17
47	0,93	Physical media	Social and behavioural privacy	4,25
48	0,88	Component testing	Installation and maintenance	4,21
49	0,84	Social and behavioural privacy	Reverse engineering of components	4,00
50	0,83	Documentation	Testing systems	3,21
51	0,68	Staff safety	Staff safety	3,04
52	0,56	Testing systems	Ethics	2,35
53	0,52	Ethics	Documentation	2,33
54	0,00	Procurement of components	Procurement of components	0,00
55	0,00	Retirement systems	Retirement systems	0,00

The importance of cyber security competences in the Slovenian economy

Motivation

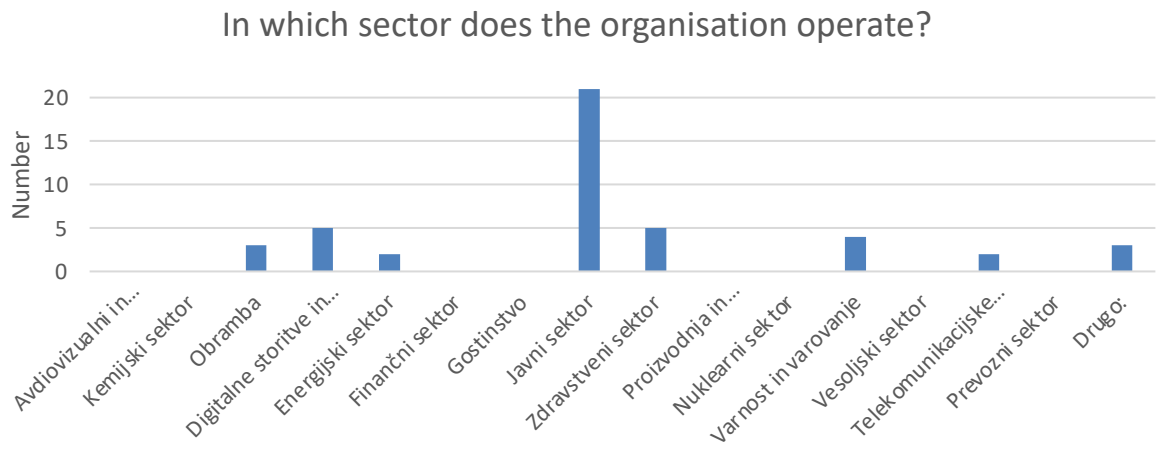
- For developing cyber security training programmes - overview of the importance of cyber security competences in the Slovenian economy
- Comparison with previous results from higher education courses and certifications

Survey

- Among organisations working on or relevant to cybersecurity
- Active from 9 February 2022 to 9 May 2022
- 45 questionnaires fully completed
- 13% response rate

Survey Participants

- Sector of the organisation



- Respondent's role in the organisation and size of the organisation

		Number of employees		
		more than 100	100 or less	Total
What is your role in the organisation?	Management staff	12	8	20
	ICT technical staff	12	8	20
	Other	3	2	5

- The average participating organisation has almost 1700 employees (from 1 to 9000)
- Most of the participating organisations have 1 person dedicated to cyber security, while the average for all respondents is 5 (0.27% of employees).

Knowledge area relevance scores

- Comparison with previous results obtained from an analysis of cyber security education (formal) and certification (informal)
- In business, human security is at the forefront of study programmes and certification, while the importance of data security and connection security is much less important

#	**Knowledge area (Economy)**	**Field of Knowledge (KF)**	**Area of expertise (Certificates)**
1	Human security	Data security	Data security
2	Organisational security	Social security	Organisational security
3	Software security	Connection security	Connection security
4	Data security	Software security	Social security
5	Social security	Security of systems	Security of systems
6	Connection security	Organisational security	Human safety
7	Security of systems	Human safety	Component safety
8	Component safety	Component safety	Software security

12 most important cybersecurity skills and competences

- Most important cyber security skills based on:
  - Analysis of study programmes
  - Analysis of certifications
  - A survey among Slovene companies/organisations

1. Network defence
2. Systems monitoring
3. Integrity and authentication
4. Access control
5. Secure communication protocols
6. Risk management
7. Security governance and policy
8. Identity management
9. Information storage security
10. Business continuity, disaster recovery and incident management
11. Cryptography
12. Privacy and security of personal data

Questions?