IT Security in Secondary CS Education: Is it missing in Today's Curricula? A Qualitative Comparison

Manuel Riel
Freie Universität Berlin
14195 Berlin, Germany
manuel.riel@fu-berlin.de

Ralf Romeike
Freie Universität Berlin
14195 Berlin, Germany
ralf.romeike@fu-berlin.de

ABSTRACT

There is a steady increase of digital networking in our world, e. g. in the form of "smart" devices as part of the internet-of-things or more recently with daily video conferences. This progress is accompanied by weekly media reports on security incidents affecting the IT we use on a daily basis. In order to provide orientation in this seemingly "insecure" digital world, it is necessary for every digital citizen to have a basic knowledge of the field of IT security. Current curricula for secondary CS education already try to cover some aspects of IT security – however, practical reports suggest that some important security-related topics have not yet been considered. Based on this assumption, we use a Qualitative Content Analysis to compare international as well as German secondary school curricula with an up-to-date body of knowledge of IT security to identify the gap to knowledge areas in current curricula.

Our results show that there is not only a lack of more in-depth topics, e. g. involving newer technologies, like internet-of-things security, the knowledge for the development of secure software – but also human factors in IT security are hardly considered in any curriculum. For further research, the results support the adjustment of relevant IT security concepts for secondary CS education.

CCS CONCEPTS

• **Social and professional topics** → **K-12 education**; • **Security and privacy** → Social aspects of security and privacy.

KEYWORDS

security, curriculum, CS education, qualitative content analysis

ACM Reference Format:
Manuel Riel and Ralf Romeike. 2020. IT Security in Secondary CS Education: Is it missing in Today's Curricula? A Qualitative Comparison. In *Workshop in Primary and Secondary Computing Education (WiPSCE '20), October 28–30, 2020, Virtual Event, Germany*. ACM, New York, NY, USA, 2 pages. https://doi.org/10.1145/3421590.3421623

1 INTRODUCTION

Media reports about IT security incidents, such as data leakage of credit card information, websites going offline due to hacking attacks, or the urgent request to update software because of an exploited vulnerability have become part of everyday life. However these security related topics do not appear to be sufficiently covered in today's curricula: Recent practical reports involving secondary schools' teachers tell that even though teenagers are said to be "tech-savvy" and tend to view hacking as "glamorous", they still lack relevant knowledge and expose themselves accidentally to online vulnerabilities [5]. Thus, we address the following research questions:

(1) What aspects regarding IT security are represented in current CS curricula (guidelines) for secondary CS education?
(2) What is the difference in topics concerning IT security between current curricula (guidelines) and foundational knowledge areas from an academic and industrial point of view?

Existing work in this area, addresses only IT security for post-secondary education: A study conducted by Hallet et al. revealed quite different foci on IT security in different curricula [3]. However, this work does not provide any implications for CS curricula in secondary education.

2 METHODOLOGY

In order to explore the questions, we adopted the research approach of a Qualitative Content Analysis by Mayring [4], which combines both qualitative and quantitative aspects. More specifically, the analysis performed by Grillenberger & Romeike for the field of data management [2] set an example for this security related investigation.

For our analysis we have chosen a broad variety of German and international secondary CS curricula and curricula guidelines in their recent version, which we will refer to as named in the following (given in the same order as in Figure 1):

- *K12*: CSTA, K-12 Computer Science Standards (revised 2017)
- *GI*: German Informatics Society, Recommended Educational Standards for lower (2008) as well as upper secondary education (2016)
- *EPA*: KMK, Uniform testing standards for CS in German high schools ("Einheitliche Prüfungsanforderungen in der Abiturprüfung", 2004)
- *EPA (v.)*: KMK, Uniform testing standards for vocational informatics in German high schools (2007)
- *BE, BY, HH, HE, NW, RP*: German secondary CS curricula for Berlin-Brandenburg, Bavaria, Hamburg, Hessen, North Rhine-Westphalia, Rhineland-Palatinate
- *AT*: Austrian Curriculum for secondary CS education ("Allgemeinbildende Höhere Schule", 2018)
- *EN*: National Curriculum in England (2013)
- *CAS*: Computing at School Curriculum (2012)

WiPSCE '20, October 28–30, 2020, Virtual Event, Germany

ACM ISBN 978-1-4503-8759-0/20/10.
https://doi.org/10.1145/3421590.3421623

Categories	CyBOK's Knowledge Areas	K12	GI	EPA	EPA (v.)	BE	BY	HH	HE	NW	RP	AT	EN	CAS	CAN	
Human, Organisational & Regulatory Aspects	Risk Management & Governance	✔	✔	✔		✔	✔			✔	✔		✔	✔	✔	71%
	Law & Regulation	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔			✔	86%
	Human Factors	✔														7%
	Privacy & Online Rights	✔		✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	93%
Attacks & Defences	Malware & Attack Technologies	✔			✔	✔	✔	✔		✔				✔		50%
	Adversarial Behaviours	✔	✔	✔			✔			✔						36%
	Security Operations & Incident Management	✔	✔	✔	✔			✔		✔					✔	50%
	Forensics															0%
Systems Security	Cryptography	✔	✔	✔		✔	✔	✔	✔	✔	✔			✔	✔	79%
	Operating Systems & Virtualisation Security															0%
	Distributed Systems Security															0%
	Authentication, Authorisation & Accountability	✔			✔										✔	21%
Software Platform Security	Software Security															0%
	Web & Mobile Security															0%
	Secure Software Lifecycle															0%
Infrastructure Security	Network Security	✔		✔	✔			✔	✔		✔	✔			✔	57%
	Hardware Security															0%
	Cyber Physical Systems															0%
	Physical Layer and Telecommunications Security															0%
	percentage coverage of KAs per curriculum:	53%	26%	37%	32%	26%	32%	32%	21%	37%	26%	16%	11%	21%	37%	29%

Figure 1: Overview of the coded results

- *CAN*: Ontario curriculum for "Science and Technology" for grade 1-8 (2007) as well as curriculum for "Technology" for grade 9-10 (2009) and grade 11-12 (2009)

The chosen deductive category system for our content analysis is the Cybersecurity Body of Knowledge (CyBOK), which aims to be a community resource being developed with consultations from academia as well as industry; its 19 knowledge areas, which are organized in five broader categories, are intended as foundational IT security basis for designing secondary to post-graduate courses [6].

Since our analysis aims to provide a broad outline of the current situation of IT security in secondary CS curricula, we coded in a simple binary way: If *any* subtopic of one of the CyBOK's 19 KAs is mentioned – no matter how minor it is treated – a checkmark for this area is noted in Figure 1. The software tool MaxQDA and its feature "lexical search" have been utilized for our content analysis and supported the efficient review of the 14 curricula (guidelines): Using a broad set of search terms, relevant text passages are automatically selected, but manually analyzed and coded if applicable.

3 RESULTS AND DISCUSSION

Our results are illustrated in Figure 1: All of the analysed curricula (guidelines) focus especially on two of the five broad categories of the CyBOK, "Human, Organisational and Regulatory Aspects" as well as "Attacks & Defences". There is little or no match on categories that may be considered more in-depth – for the big exception of cryptography, which is included in the majority of curricula analysed. This appears to support the teachers' impression from Pencheva et al. that more "technical" knowledge regarding IT security is outside the scope [5]. A big gap to academia and industry becomes apparent here.

While these results have not been unexpected, one point, however, is surprising: The knowledge area "Human Factors", which also involves current IT security keywords like "social engineering" and "security awareness", is only - and there just even slightly – considered in one curriculum. Human behaviour itself is often viewed as a major, if not the most serious, risk for IT systems by experts and therefore has already been considered in the context of big ideas for CS education [1].

We need to emphasize that taking a short view on Figure 1 might distort one's impression: It is important to keep our binary coding system in mind; every knowledge area summarizes many subtopics, therefore a checkmark in one cell in Figure 1 does not mean that the corresponding curriculum contains all of the knowledge area's subjects, but involves *any* of its topics at *any* level; e. g. the knowledge area "Risk Management & Governance" is mentioned in most curricula, but all of them keep the term "risk" at a very intuitive level , often without any probabilistic considerations of occurrence or any assessment of the potential extent of damage. A reasonable, in-depth risk analysis of threats in real-life situations is missing in all curricula.

4 CONCLUSION

Our analysis provides insights about the status of IT security and its representation in today's curricula – and how it compares to a body of foundational knowledge from a scientific view. Our further research on IT security in secondary education will focus on exploring security related topics, which are important for every student, every teacher, every member of today's digital world.

REFERENCES

[1] Tim Bell, Paul Tymann, and Amiram Yehudai. 2011. The Big Ideas of K-12 Computer Science Education.

[2] Andreas Grillenberger and Ralf Romeike. 2014. A comparison of the field data management and its representation in secondary CS curricula. In *Proceedings of the 9th Workshop in Primary and Secondary Computing Education*. 29–36.

[3] Joseph Hallett, Robert Larson, and Awais Rashid. 2018. Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. In *2018 {USENIX} Workshop on Advances in Security Education ({ASE} 18)*.

[4] Philipp Mayring. 2004. Qualitative content analysis. *A companion to qualitative research* 1, 2004 (2004), 159–176.

[5] Denny Pencheva, Joseph Hallett, and Awais Rashid. 2020. Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy* 18, 2 (2020), 68–74.

[6] Awais Rashid, George Danezis, Howard Chivers, Emil Lupu, Andrew Martin, Makayla Lewis, and Claudia Peersman. 2018. Scoping the cyber security body of knowledge. *IEEE Security & Privacy* 16, 3 (2018), 96–102.