Horizon 2020 Program (2014-2020)
Cybersecurity, Trustworthy ICT Research & Innovation Actions
Security-by-design for end-to-end security
H2020-SU-ICT-03-2018

CONCORDIA

Cyber security cOmpeteNCe fOr Research anD InnovAtion

Work Package 5: Exploitation, dissemination, certification and standardization

REPORT ON SME CYBERSECURITYSTANDARDS

Abstract: This document describes the methodology and results on cybersecurity standards for SMEs. The document concludes with recommendations and directions for development of future cybersecurity standards and frameworks targeting SMEs.

Actual date of delivery:
24/03/20223

Deliverable dissemination level:
Public

Contributors:
Argyro Chatzopoulou (TÜV TRUST IT)
Muriel Franco (UZH)

This project has received funding
from the European Union's Horizon 2020 research and innovation programme
under grant agreement No 830927.

THE CONCORDIA CONSORTIUM

UniBW/CODE	University Bundeswehr Munich / Research Institute CODE (Coordinator)	Germany
FORTH	Foundation for Research and Technology - Hellas	Greece
UT	University of Twente	Netherlands
SnT	University of Luxembourg	Luxembourg
UL	University of Lorraine	France
UM	University of Maribor	Slovenia
UZH	University of Zurich	Switzerland
JACOBSUNI	Jacobs University Bremen	Germany
UI	University of Insubria	Italy
CUT	Cyprus University of Technology	Cyprus
UP	University of Patras	Greece
TUBS	Technical University of Braunschweig	Germany
TUDA	Technical University of Darmstadt	Germany
MU	Masaryk University	Czech Republic
BGU	Ben-Gurion University	Israel
OsloMET	Oslo Metropolitan University	Norway
Imperial	Imperial College London	UK
UMIL	University of Milan	Italy
BADW-LRZ	Leibniz Supercomputing Centre	Germany
EIT DIGITAL	EIT DIGITAL	Belgium
TELENOR ASA	Telenor ASA	Norway
ADS	Airbus Defence and Space GmbH (as a replacement for Airbus Protect GmbH)	Germany
SECUNET	secunet Security Networks AG	Germany
IFAG	Infineon Technologies AG	Germany
SIDN	Stichting Internet Domeinregistratie Nederland	Netherlands
SURF	SURF BV	Netherlands
CYBER-DETECT	Cyber-Detect	France
TID	Telefonica I+D SA	Spain
RUAG	RUAG AG (as a replacement for RUAG Schweiz AG)	Switzerland
BITDEFENDER	Bitdefender SRL	Romania
ATOS	Atos Spain S.A.	Spain
SAG	Siemens AG	Germany
Flowmon	Flowmon Networks AS	Czech Republic
TÜV TRUST IT	TUV TRUST IT GmbH	Germany
TI	Telecom Italia SPA	Italy

Efacec	EFACEC Electric Mobility SA (as a replacement for EFACEC Energia)	Portugal
ARTHUR'S LEGAL	Arthur's Legal B.V.	Netherlands
eesy-inno	eesy-innovation GmbH	Germany
DFN-CERT	DFN-CERT Services GmbH	Germany
CXB	CaixaBank SA	Spain
BMW Group	Bayerische Motoren Werke AG	Germany
NCSA	Ministry of Digital Governance - National Cyber Security Authority	Greece
RISE	RISE Research Institutes of Sweden AB	Sweden
Ericsson	Ericsson AB	Sweden
SBA	SBA Research gemeinnutzige GmbH	Austria
IJS	Institut Jozef Stefan	Slovenia
UiO	University of Oslo	Norway
ULANC	University of Lancaster	UK
ISI	ATHINA-ISI	Greece
UNI PASSAU	University of Passau	Germany
RUB	Ruhr University Bochum	Germany
CRF	Centro Ricerche Fiat	Italy
ELTE	EOTVOS LORAND TUDOMANYEGYETEM	Hungary
Utimaco	Utimaco Management GmbH	Germany
FER	University of Zagreb, Faculty of Electrical Engineering and Computing	Croatia
ICENT	Innovation Centre Nikola Tesla	Croatia
Utilis	Utilis d.o.o	Croatia
Polito	Politecnico di Torino	Italy

CONTENTS

1. Introduction 5

1.1. Purpose of this Report 5

1.2. Methodology 6

1.2.1. Part 1: Literature Review 6

1.2.2. Part 2: Analysis of Selected Publications 6

2. Results and Discussion 6

3. Conclusions & Recommendations 11

1. INTRODUCTION

mall and Medium-sized Enterprises (SMEs) are the backbone of the EU's economy. They represent 99% of all businesses in the EU and employ around 100 million people. They also account for more than half of Europe's GDP and play a key role in adding value to all sectors of the EU economy. They serve both as enablers for the digital transformation and as a core element of the EU social fabric1.

The ENISA Report „Cybersecurity for SMEs"2, provides insights on the relationship of European SMEs with digital tools and the challenges faced. For example, the majority of the European SMEs that participated in the survey, use various information services as part of their daily business operations (e.g. Teleworking, e-banking, email and communication services) and 85% of the organisations have identified cybersecurity as a key concern.

Contrary to a concept that cyber-attacks occur only to large organisations, all enterprises can be attacked regardless of their size and stored information.

Within this report, seven categories of major challenges for SMEs have been identified:

- low cybersecurity awareness of the personnel,
- inadequate protection of critical and sensitive information,
- lack of budget,
- lack of ICT cybersecurity specialists,
- lack of suitable cybersecurity guidelines specific to SMEs,
- shadow IT, i.e. shift of work in ICT environment out of SME's control,
- low management support.

The ENISA Report concludes with recommendations and guidance at a company, national and European level. On the other hand, as part of the CONCORDIA project Task T4.3, a methodology for cybersecurity planning and investment has been proposed, as a way to further assist and guide SMEs regarding cybersecurity.

1.1. PURPOSE OF THIS REPORT

A team comprising of members from Task 4.3 (Economics) and Task 5. 3. (Certification and Standardisation), took the recommendations of the ENISA reports[1],[2] and sought out to investigate if such guidelines, templates and standards exist and whether they are in line with the relevant results of the CONCORDIA project.

The CONCORDIA team, following the methodology presented in Section 1.2, analysed existing standards and publications to identify relevant characteristics and differences of current literature. Based on that, a set of recommendations is provided for the next generation of standards.

1 https://www.enisa.europa.eu/topics/cybersecurity-education/sme_cybersecurity & https://single-market-economy.ec.europa.eu/smes_en

2 https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes

1.2. METHODOLOGY

The CONCORDIA project team designed the following methodology, divided in two parts, in order to achieve the objectives mentioned in section 1. 1. (Purpose) above.

1.2.1. PART 1: LITERATURE REVIEW

The first part of the methodology, focused on the identification of applicable publications (Standards, Certification Schemes, guides or Reports) specific and focused on cybersecurity and SMEs. In order to have a basis for comparison, regarding the areas covered, the rationale and the magnitude of the SME publication, during this part, a sample of cybersecurity standards not focused on SMEs were also identified. Since the number of this latter category is very big, the team decided to only sample some that are recognized internationally.

1.2.2. PART 2: ANALYSIS OF SELECTED PUBLICATIONS

The second part of the methodology, focused on the analysis of the identified publications (from the first part). This analysis aimed on the identification of the areas covered by each publication and whether the publications depict different cybersecurity maturity levels.

The CONCORDIA team went through all of the identified publications, identified the number and content of the areas covered by each publication and recorded the results in a suitable file.

2. RESULTS AND DISCUSSION

This section presents the results of the results obtained by applying the methodology, thus, showing the findings of the identification and analysis of publications available for SMEs. Also, the Cybersecurity Technical and Economic Approach (CyberTEA) is introduced as contribution of the CONCORDIA project to simplify the cybersecurity planning and investment for SMEs.

Identification and Analysis results

The CONCORDIA team identified 24 distinct publications containing guidelines, recommendations and requirements on cybersecurity. 17 of these publications were identified as SME specific and 7 as (generic) non SME specific.

Table 1, depicts the list of the identified (by the project team) cybersecurity publications containing recommendations, guidelines and requirements mainly for SMEs and secondarily in general.

Table 2, depicts the number of cybersecurity recommendations, guidelines and requirements areas identified within the publications of Table 1. For each one of the publications, the information depicted is: the number of areas covered, if the publication is SME specific and the number of levels (from a cybersecurity maturity point of view) identified.

Table 1: Identified cybersecurity publications

Publication Title	Issuing Entity	Year of Publication	Link
Cybersecurity for SMEs - Challenges and Recommendations	ENISA	2021	https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes
Small Business Guide: Cyber Security	National Cyber Security Centre (UK)	2020	https://www.ncsc.gov.uk/collection/small-business-guide
Cyber Security Guide for SME	The Centre for Cyber Security Belgium	2020	https://ccb.belgium.be/en/document/guide-sme
SME Guide on Information Security Controls	European Digital SME Alliance	2022	https://www.digitalsme.eu/digital/uploads/SME-ISC-Guide.pdf
Framework for Improving Critical Infrastructure Cybersecurity (version 1. 1.)	National Institute of Standards and Technology (NIST)	2018	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
MANUFACTURERS GUIDE TO CYBERSECURITY For Small and Medium-Sized Manufacturers	THE MEP NATIONAL NETWORK	2019	https://www.nist.gov/system/files/documents/2019/11/14/mepnn_cybersecurity_guide_10919-508.pdf
Cyber Guidance for Small Businesses	Cybersecurity & Infrastructure Security Agency (US)	2023	https://www.cisa.gov/cyber-guidance-small-businesses
Cybersecurity for SMEs. Part 1: Cybersecurity Standardisation Essentials.	ETSI	2021	https://www.etsi.org/deliver/etsi_tr/103700_103799/10378701/01. 01. 01_60/tr_10378701v010101p.pdf
10 STEPS FOR A CYBERSECURITY-BEGINNER SME	Cyberwatching.eu	2021	https://cyberwatching.eu/smes-guides/10-steps-cybersecurity-beginner-sme
Cybersecurity guide for SMEs	ENISA	2022	https://gcatoolkit.org/wp-content/uploads/2022/03/ENISA-Cybersecurity-guide-for-SMEs-online-single_page.pdf
Cyber Security: Small Business Guide	National Cyber Security Centre (UK)	2017	https://nbcc.police.uk/images/guidance/Cyber_Security_-_Small_Business_Guide_NCSC.pdf
SME Guide on Information Security Management: the standard ISO27001 made easy for SMEs	European Digital SME Alliance - Small Business Standards	2018	https://www.digitalsme.eu/new-sbs-guide-information-security-management-standard-iso27001-made-easy-smes/
Cyber Security Planning Guide	Federal Communication Commission	2023	https://www.fcc.gov/cyberplanner
SMALL FIRMS CYBERSECURITY GUIDANCE HOW TO CONSUME THREAT INFORMATION FROM THE FS-ISAC	FS-ISAC	2017	https://www.sifma.org/wp-content/uploads/2017/07/small-firms-cybersecurity-guide-2017-1.pdf
ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	ISO/IEC	2022	https://www.iso.org/standard/82875.html
ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls	ISO/IEC	2022	https://www.iso.org/standard/75652.html

Publication Title	Issuing Entity	Year of Publication	Link
Security and Privacy Controls for Information Systems and Organizations (NIST 800-53, Rev.5)	National Institute of Standards and Technology (NIST)	2020	https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final
Q & A Guide. Promoting Cybersecurity for SMEs in Europe	Huawei Technologies Co., Ltd, Global Digital Foundation, eit Digital	2023	https://www-file.huawei.com/-/media/corp2020/media-center/pdf/facts/papers/cybersecurity%20for%20european%20smes%20a%20huawei%20study.pdf?la=en
NISTIR 7621, Revision 1, Small Business Information Security: The Fundamentals	National Institute of Standards and Technology (NIST)	2016	https://nvlpubs.nist.gov/nistpubs/ir/2016/nist.ir.7621r1.pdf
Cyber Essentials: Requirements for IT infrastructure v3. 1.	Narional Cyber Security Centre (UK)	2023	https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-January-2023.pdf
KSV1870 Cyber Risk B Rating, Cyber TRUST Austria - Label	KSÖ	2023	https://cyberrisk-rating.at/cyber-risk-2023-schema-en.pdf
Portuguese Normative Document - Technical Specification, DNP TS 4577-1 2021, Digital Maturity - Digital Seal. Part 1: Cybersecurity	Instituto Portugues da Qualidade	2021	Not available online
CIS Controls	Center for Internet Security (CIS) Controls (USA)	2021	https://www.cisecurity.org/controls

Table 2: Analysis results of identified cybersecurity publications

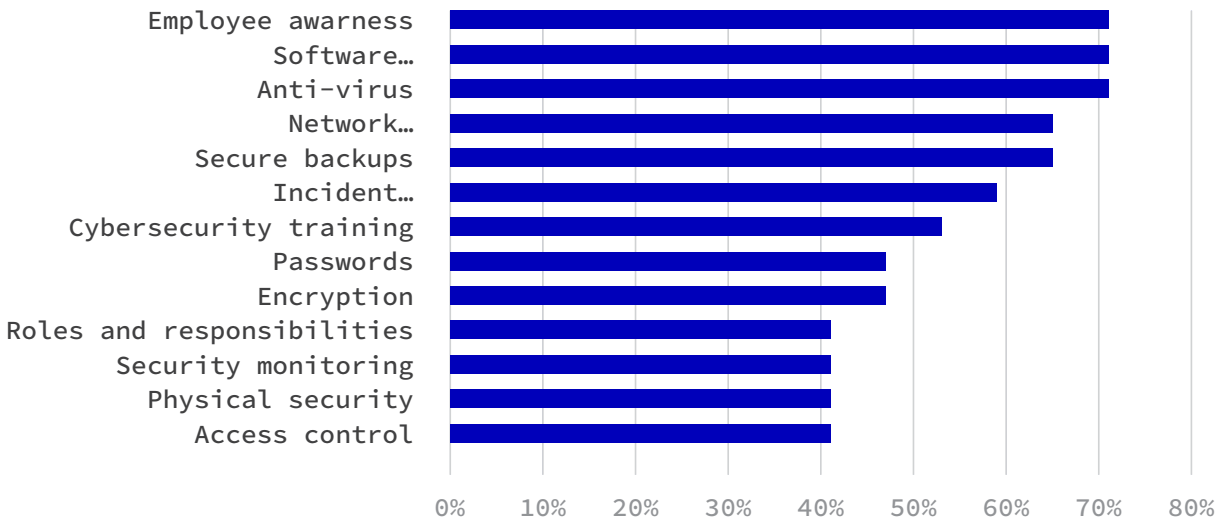
Publication Title	Number of Areas Covered	Is SME Specific	Number of Levels Identified
Cybersecurity for SMEs - Challenges and Recommendations	18	Yes	1
Small Business Guide: Cyber Security	10	Yes	1
Cyber Security Guide for SME	52	Yes	1
SME Guide on Information Security Controls	35	Yes	1
Framework for Improving Critical Infrastructure Cybersecurity (version 1. 1.)	50	No	1
MANUFACTURERS GUIDE TO CYBERSECURITY For Small and Medium-Sized Manufacturers	21	Yes	1
Cyber Guidance for Small Businesses	7	Yes	1
Cybersecurity for SMEs. Part 1: Cybersecurity Standardisation Essentials.	7	Yes	1
10 STEPS FOR A CYBERSECURITY-BEGINNER SME	14	Yes	1
Cybersecurity guide for SMEs	22	Yes	1
Cyber Security: Small Business Guide	13	Yes	1
SME Guide on Information Security Management: the standard ISO27001 made easy for SMEs	47	Yes	2
Cyber Security Planning Guide	38	No	1

Publication Title	Number of Areas Covered	Is SME Specific	Number of Levels Identified
SMALL FIRMS CYBERSECURITY GUIDANCE HOW TO CONSUME THREAT INFORMATION FROM THE FS-ISAC	18	Yes	5
ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements	60	No	1
ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls	49	No	1
Security and Privacy Controls for Information Systems and Organizations (NIST 800-53, Rev.5)	83	No	1
Q & A Guide. Promoting Cybersecurity for SMEs in Europe	17	Yes	1
NISTIR 7621, Revision 1, Small Business Information Security: The Fundamentals	27	Yes	1
Cyber Essentials: Requirements for IT infrastructure v3. 1.	11	Yes	1
KSV1870 Cyber Risk B Rating, Cyber TRUST Austria - Label	20	Yes	1 (for SMEs)
Portuguese Normative Document - Technical Specification, DNP TS 4577-1 2021, Digital Maturity - Digital Seal. Part 1: Cybersecurity	35	Yes	3
CIS Controls	32	No	3

The analysis of the identified publications revealed, 88 distinct areas. The areas include all categories of controls (organizations, technological, physical and people) with different range and strength. In some cases, the areas are generic (covering the basic level of protection) and in some cases the areas are specialized (covering more advanced controls).

The areas covered by the majority of SME specific publications are highlighted in Figure 1.

Figure 1: Areas covered by the majority of publications



As shown, most of the identified SME specific publications focus on basic security (e.g., employee awareness, software patches, anti-virus, and backups). Some of the SME specific publications also focus on technical elements like encryption, security monitoring, and access control. However, none of the standards analysed explicitly mention economic aspects, such as cost management and cyber insurance and only a limited few reference (even at a basic level risk management).

When comparing these results with those of the 7 non SME specific publications, the following conclusions are deduced:

- The non SME specific publications cover more areas, and in most cases at a different level of detail or level of security.
- The non SME specific publications identify Risk Assessment, Risk Management and Cyber Insurance as mandatory or optional (the latter) controls.
- The subject of cybersecurity economics is not directly mentioned within any of the identified non SME specific publications.
- The CONCORDIA CyberTEA

CONCORDIA worked on different fronts in order to address some of the gaps of cybersecurity planning identified along the project and to satisfy and highlight requirements not covered by current frameworks and standards. As an outcome of CONCORDIA Task T4.3, the CyberTEA approach3 was proposed as a methodology for cybersecurity planning and investment that puts cost management also as a pillar of the definition of a cybersecurity strategy. CyberTEA is a five phase-based approach composed by the following phases:

- Understanding of business profile,
- Risk management,
- Cybersecurity requirements,
- Cost management, and
- Effective deployment.

CyberTEA shows that there should be a direct correlation between cost and benefit, expressed in simple business and economic/financial terms, behind the implementation of a cybersecurity strategy of an organization. When this methodology is compared to the outcomes of the analysis conducted in Section 2, it is possible to identify a set of limitations and challenges still open in the current literature. The cybersecurity recommendations, guidelines, and requirements for SMEs are formulated as a predetermined one-size-fits-all set of controls. The **business profile**, the complexity or criticality of the services of the SMEs or the relevant size and digitization of the SMEs are not taken into consideration when deciding upon the controls. **Risk assessment** is not, in most cases, the core tool for decision-making on which controls to apply, and **Cost management** is not utilized to select which solution achieves the required level of security within the allocated / available budget.

As described within the CONCORDIA CyberTEA approach3 documentation, for a cybersecurity implementation to be successful and adapted to the needs (in-

3 Muriel Franco: *CyberTEA: a Technical and Economic Approach for Cybersecurity Planning and Investment*; Universität Zürich, Communication Systems Group, Department of Informatics, Zürich, Switzerland, February 2023, Available at: *https://figueredofranco.com/static/files/PhD-M-Franco.pdf*

cluding technical, economic, and legal) of the organization, all key five phases determined by CyberTEA need to be followed even that specific tasks might be optional according to the technical expertise and demands of the company. The absence of critical phases in the cybersecurity compliance journey of SMEs raises serious concerns about whether such approaches are really effective or just provide a false sense of security.

3. CONCLUSIONS & RECOMMENDATIONS

Based on the analysis conducted on identified cybersecurity publications, it was possible to identify and highlight the big picture of current approaches as well as obtain insights about possible further next steps. The findings are summarised as follows:

Most (more than half of the analysed SME specific publications) include the following areas within their recommendations: Employee awareness, Software patches, Anti-Virus, Network Security (e.g. Firewalls), Secure Backups, incident Planning and response procedures and Cybersecurity training.

Risk Management (even at a basic level) is part of only 24% of the analysed SME specific publications.

Risk Management (even at a basic level) is part of more than 70% of the analysed non SME specific publications.

The contents of the SME specific publications are presented as a one size fits all solution without (in most cases) taking into consideration the context of the organization.

The economics/cost management subject is not introduced explicitly in any of the publications analysed. There is a reference in some cases of the need to analyse the organisation, the needs, the objectives, the compliance requirements and the information, the implementation of controls following a risk assessment process, but there is no concrete information on how economics can play a role within this decision making.

It is the opinion of the CONCORDIA project that risk management is a critical tool in the identification and customization of the measures/controls to be implemented, which is currently being neglected in the case of the analysed SME-specific publications and recommendations. It is critical to support companies to invest effectively in cybersecurity, even when in-house technical expertise is unavailable. Therefore, different multidisciplinary approaches must be considered, including economic models to support cybersecurity decision-making. Different guidelines support SMEs in implementing at least a basic level of cybersecurity controls. However, there should be a clear indication that these controls should be an initial step for achieving a cybersecurity strategy, which should be reviewed and evolved continuously.

Publications providing cybersecurity recommendations, guidelines, or require-

ments for SMEs should also include a mandatory step where each organization identifies the business context and the criticality of their information and services. The results of this step should contribute to the decision of which controls and to what extent should be implemented by the SME. To further assist in the identification of possible controls, SME-specific cybersecurity capability maturity models could be created. The models could indicate controls of different security strengths based on the SMEs' needs and thus provide useful guidance adapted to the organization's needs. It should be noted at this point that 4 of the 17 identified cybersecurity SME-specific publications incorporate multiple (more than 1) levels. However, currently, there is no uniform way or concrete indication of when and why an SME should implement which level.


CONCORDIA
Cyber security cOmpeteNCe fOr Research anD InnovAtion