DOI: 10.2507/37th.daaam.proceedings.xxx

CYBERSECURITY PRACTICES AND REPORTED ICT SECURITY INCIDENT CONSEQUENCES IN EUROPEAN ENTERPRISES: A BUSINESS AND ECONOMIC PERSPECTIVE

Berislav Andrlić, Ivan Jajić, Božidar Jaković, Luka Madžarević

Working Paper of 37th DAAAM Symposium

This Publication has to be referred as: Andrlić, B[erislav]; Jajić, I[van]; Jaković B[ožidar] & Madžarević, L[uka] (2026). Cybersecurity Practices and Reported ICT Security Incident Consequences in European Enterprises: A Business and Economic Perspective, Proceedings of the 37th DAAAM International Symposium, pp.xxxx-xxxx, B. Katalinic (Ed.), Published by DAAAM International, ISBN 978-3-902734-xx-x, ISSN 1726-9679, Vienna, Austria
DOI: 10.2507/37th.daaam.proceedings.xxx

Abstract

This paper examines whether broader use of cybersecurity practices is associated with lower reported consequences from Information and Communications Technology (ICT) security incidents across European Union enterprises. Using open Eurostat data for all 27 EU Member States, the study combines three country-level indicators, use of at least one ICT security measure, staff awareness of ICT security obligations, and ICT security documentation into a standardised Cybersecurity Practice Index (CPI). The outcome is the share of enterprises that experienced consequences from ICT security incidents in 2023. Security practices are widespread, 92.76% of EU enterprises used at least one security measure, 59.97% made staff aware of security obligations, and 35.50% had security documentation, while 21.54% reported incident consequences. Across countries, the CPI is positively rather than negatively associated with reported incident consequences (Pearson r = 0.43). The baseline regression estimates a 3.25 percentage-point increase in reported incident consequences per one-standard-deviation increase in the CPI (p = 0.079). The results suggest that reported incident consequences should not be interpreted as a simple inverse measure of cybersecurity effectiveness, because digital exposure, incident detection, reporting differences and post-incident responses may also affect the observed country-level patterns.

Keywords: cybersecurity practices; ICT security incidents; incident consequences; Eurostat; business informatics; regression analysis

1. Introduction

Digitalised enterprises depend on connected information systems, cloud services and data-intensive processes, which makes cybersecurity an operational business issue rather than only a technical one. Cybersecurity is also closely linked to Industry 4.0 and enterprise digital transformation [1]. Recent research stresses that effective cybersecurity combines technical controls with employee awareness, organisational routines and management practices [2], [3], while cyber incidents can have direct operational and economic consequences [4], [5].

The empirical question in this paper is therefore, do countries in which enterprises report broader use of cybersecurity practices also report fewer consequences from ICT security incidents? Eurostat open data allow this question to be examined consistently across the EU, while also showing why incident reporting must be interpreted carefully.

RQ1: How widely are basic cybersecurity, staff-awareness and governance practices used across EU enterprises?

RQ2: Is higher cybersecurity practice intensity associated with lower reported consequences from ICT security incidents across EU countries?

RQ3: Do the results support treating reported incident consequences as a straightforward indicator of weaker cybersecurity?

2. Literature review

Recent literature treats cybersecurity as a combination of technical, organisational and human capabilities. Knowledge management and staff awareness are important because security controls depend on employees understanding and applying security obligations [2], [3]. At the same time, enterprises differ in resources, digital exposure and cybersecurity investment, which can influence both actual risk and the probability that incidents are detected and reported [4]. European Union Agency for Cybersecurity (ENISA) also emphasises the continuing operational relevance of cyber threats for European organisations [5]. These arguments motivate an empirical design that separates security-practice intensity from reported incident consequences instead of assuming that more reported incidents automatically imply weaker cybersecurity. Recent studies on phishing also suggest that there is an imbalance between the emphasis on technical aspects of detection and the human factors, thus highlighting the need to raise staff awareness to counter this form of cyber-security threat [11].

3. Materials and Methods

3.1. Research design

The study uses a quantitative cross-sectional design based entirely on public Eurostat data [10]. The unit of analysis is an EU Member State. All 27 Member States are included in the main analysis, so the country sample is complete for the three main cybersecurity-practice indicators and the incident outcome. The analysis estimates associations between country-level enterprise indicators and does not claim firm-level or causal effects.

3.2. Data source and sample

The data come from Eurostat indicators on ICT security in enterprises [6], [7], [8]. The 2024 sample includes enterprises with 10 or more employees or self-employed persons in NACE Rev. 2 sections C to J, L to N, and group 95.1. Cybersecurity-practice indicators refer to 2024, whereas incident consequences refer to 2023. Therefore, the analysis cannot determine whether the measured practices prevented the reported incidents. Instead, the regression assesses the associations between countries' cybersecurity-practice levels in 2024 and the reported incident consequences in 2023. It includes enterprises of various activity types beyond manufacturing organizations.

Variable	Eurostat table	Operational definition	Use
Security measure use	isoc_cisce_ra	Enterprises using at least one ICT security measure	Main CPI component
Staff awareness	isoc_cisce_ra	Enterprises making staff aware of ICT security obligations	Main CPI component
Security documentation	isoc_cisce_ra	Enterprises with documents on ICT security measures/practices	Main CPI component
Recent documentation	isoc_cisce_ra	Security documents defined/reviewed in previous 12 months	Sensitivity check; n = 20
Incident consequences	isoc_cisce_ic	Enterprises with ICT security incidents leading to consequences in 2023	Dependent variable

Table 1. Variables and Eurostat sources used in the analysis

3.3. Measurement

The dependent variable is the share of enterprises that reported consequences from at least one ICT security incident in 2023. The Cybersecurity Practice Index (CPI) is based on three indicators, the use of at least one ICT security measure, staff awareness of ICT security obligations and ICT security documentation. Each indicator is standardised and the three

Working Paper of 37th DAAAM Symposium

values are averaged. The resulting index is again standardised, thus a higher CPI means a wider use of cybersecurity practices compared to other EU countries. The indicator on documents reviewed within the previous 12 months is not included in the main CPI because Eurostat reports missing values for seven EU countries; it is used only as a sensitivity check.

3.4. Statistical analysis

The analysis is based on descriptive statistics and on Pearson and Spearman correlations. The primary regression is an OLS regression of reported incident consequences on the CPI, using robust standard errors [9]. Additional regressions split the three CPI components apart. Robustness is checked by re-estimating the CPI regression 27 times, dropping one country each time, and testing the recent-documentation indicator on the smaller 20-country sample. All findings are interpreted as country-level associations and not as causal effects.

3.5. Reproducibility and limitations

All inputs are public Eurostat statistics and can be reconstructed using the dataset codes and definitions in Table 1. The approach follows Eurostat methodological guidance for enterprise ICT statistics [6]. The main limitation is aggregation, country-level percentages cannot identify whether a specific security measure prevented an incident in a specific enterprise. Countries with greater digital exposure, stronger monitoring or better reporting procedures may record more incidents even when their cybersecurity practices are more mature. For this reason, the analysis is used for cross-country benchmarking and association, not causal evaluation.

4. Results

4.1. Descriptive results

Cybersecurity practices are widespread in the EU, but there is substantial cross-country variation. Eurostat reports that 92.76% of EU enterprises used at least one ICT security measure in 2024, 59.97% made employees aware of ICT security obligations, 35.50% had ICT security documentation, and 21.82% had defined or reviewed such documentation within the previous 12 months. At the same time, 21.54% of EU enterprises experienced consequences from ICT security incidents in 2023 [7], [8]. Figure 1 summarises these EU-level benchmarks.

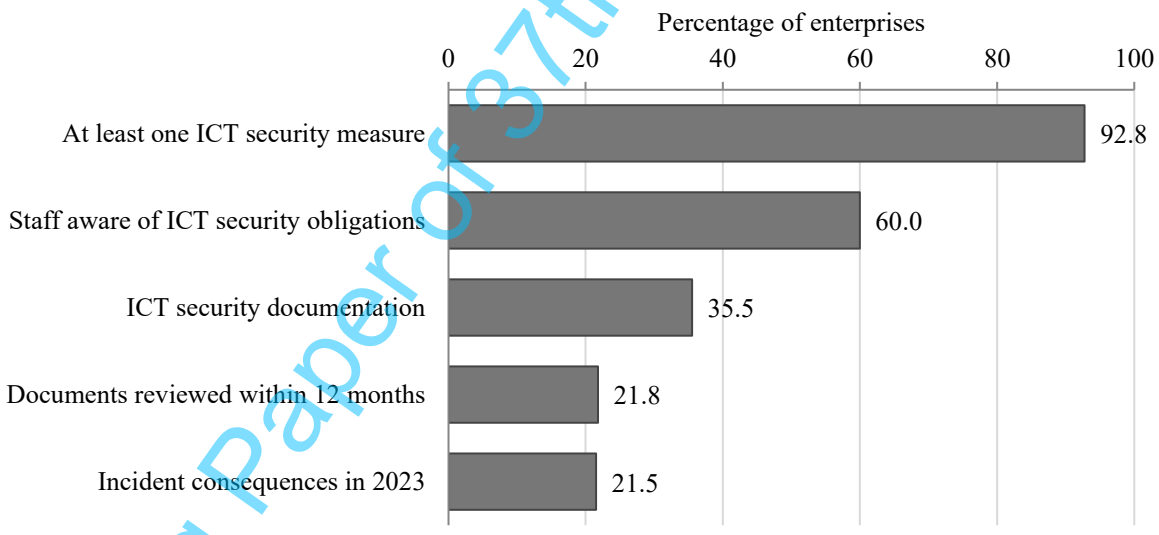

Fig. 1. EU enterprise cybersecurity indicators from the Eurostat 2024 collection; incident consequences refer to 2023.

The unweighted country averages differ from the EU aggregate because Eurostat aggregates are weighted by enterprise populations. Across the 27 countries, the average share using at least one security measure is 91.02%, while the average share reporting incident consequences is 19.85%. Greece has the lowest share using at least one measure (71.84%), whereas Finland has the highest (98.74%). Staff awareness ranges from 31.68% in Greece to 77.47% in Czechia, and security documentation ranges from 13.67% in Bulgaria to 59.41% in Finland. Incident consequences range from 11.52% in Austria to 42.20% in Finland.

Indicator	N	Mean	SD	Min	Max
At least one security measure	27	91.02	5.69	71.84	98.74

Working Paper of 37th DAAAM Symposium

Indicator	N	Mean	SD	Min	Max
Staff awareness	27	58.34	10.67	31.68	77.47
Security documentation	27	36.25	12.40	13.67	59.41
Recent security documentation	20	20.88	9.33	8.20	42.01
Incident consequences	27	19.85	7.64	11.52	42.20

Table 2. Descriptive statistics across EU Member States

4.2. Association between cybersecurity practices and incident consequences

The cross-country pattern does not show the expected simple negative relationship. The CPI is positively correlated with reported incident consequences (Pearson r = 0.43, p = 0.024; Spearman rho = 0.42, p = 0.027). Among the three components, use of at least one security measure has a Pearson correlation of 0.45 (p = 0.020), staff awareness 0.29 (p = 0.148), and security documentation 0.38 (p = 0.048). Figure 2 shows the positive country-level relationship between the composite index and reported incident consequences.

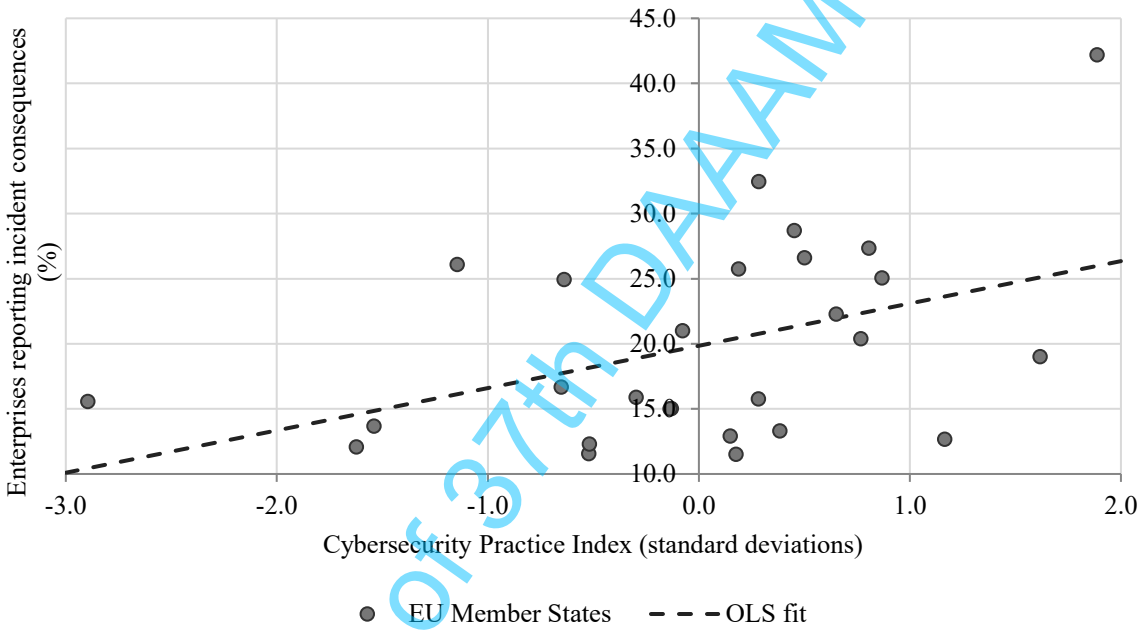

Fig. 2. Cybersecurity Practice Index and reported ICT security incident consequences across EU Member States

4.3. Regression and robustness results

The baseline OLS model produces a positive CPI coefficient of 3.25 percentage points (HC3 robust SE = 1.85, p = 0.079, R-squared = 0.188). Thus, a one-standard-deviation higher CPI is associated with approximately 3.25 percentage points more enterprises reporting incident consequences. The coefficient is not statistically significant at the usual 5% level. However, the positive direction does not lend support to the simple expectation that countries with wider cybersecurity practices necessarily report fewer incident consequences.

Model	Explanatory variable	Coef.	Robust SE	p	R2	N
M1	CPI (standardised)	3.25	1.85	0.079	0.188	27
M2	At least one security measure	0.60	0.39	0.125	0.200	27
M3	Staff awareness	0.20	0.16	0.212	0.082	27

Working Paper of 37th DAAAM Symposium

Model	Explanatory variable	Coef.	Robust SE	p	R2	N
M4	Security documentation	0.24	0.15	0.121	0.147	27

Table 3. OLS regressions of reported incident consequences

Robustness checks support the stability of this direction. In the leave-one-country-out analysis, the coefficient on CPI was positive in all 27 re-estimations and ranged from 1.89 to 4.09 percentage points. The separate regressions for the three components of the CPI were also positive, but none was statistically significant at the 5% level. The recent-documentation indicator was positive but not statistically significant (β=0.17, p=0.452) and was available for 20 countries. Therefore, the positive direction of the relationship was not driven by a single country or one specific CPI component.

5. Discussion

The main finding is not that cybersecurity practices increase cyber risk. Rather, the open data show that countries with broader reported use of cybersecurity practices do not necessarily report fewer incident consequences. This is plausible because cybersecurity maturity, digital exposure and incident visibility move together. Enterprises that operate more digital systems may face a larger attack surface, while stronger monitoring and governance can increase the probability that incidents are detected and recorded. Another possible explanation is the timing of the indicators. Cybersecurity practices are measured in 2024, whereas incident consequences are in 2023. Therefore, some organizations may have strenghtend their cybersecurity practices after experiencing an incident. Because the data are aggregate, this potential response effect cannot be separated out from a preventive effect. The positive association therefore highlights a measurement problem, reported incident consequences are not a direct inverse measure of cybersecurity effectiveness.

6. Conclusion

Based on harmonised Eurostat data for all 27 EU Member States, the paper finds that the use of cybersecurity practices is high but uneven and that there are substantial differences in reported consequences of information and communications technology security incidents. This assessment is based on harmonized Eurostat data. The primary regression coefficient of the Cybersecurity Practice Index is not statistically significant at the 5% level but positively associated with the reported incident consequences. This is not proof that cybersecurity practices increase cyber risk. Rather, it is indicative that the consequences of the incident reported can only be understood by considering differences in digital exposure, incident detection, reporting practices and potential security responses that may be enacted following an incident.

From a business informatics perspective, cybersecurity performance should not be evaluated solely on the basis of incident counts, but together with broader operational risk indicators. Enterprise boards and senior management should not look at the number of incidents reported as the only measure of the performance of the person responsible for information security or of the return on investment for cybersecurity. A more thorough assessment should also include the level of digital exposure, the time it takes to detect and respond to incidents, the time it takes to recover operations, service continuity, and the extent of losses. For researchers, the results highlight the need for firm-level and longitudinal data that would allow preventive effects, post-incident responses, exposure and reporting practices to be examined separately.

7. References

[1] Vranakova, N. & Gyurak Babelova, Z. (2024). Insights into Industry 4.0 Components and Acceptance of New Technologies in Industrial Enterprises, Proceedings of the 35th DAAAM International Symposium, pp.0292-0298, B. Katalinic (Ed.), DAAAM International, Vienna, Austria, ISBN 978-3-902734-44-0, ISSN 1726-9679, DOI: 10.2507/35th.daaam.proceedings.040

[2] Albrecht, J.; Dostalova, P.; Kralik, L. & Kralickova, G. (2023). Benefits of Knowledge Management in Cybersecurity - Initial Study, Proceedings of the 34th DAAAM International Symposium, pp.0526-0530, B. Katalinic (Ed.), DAAAM International, Vienna, Austria, ISBN 978-3-902734-41-9, ISSN 1726-9679, DOI: 10.2507/34th.daaam.proceedings.069

[3] Chaudhary, S.; Gkioulos, V. & Katsikas, S. (2023). A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises, Computer Science Review, Vol. 50, 100592, DOI: 10.1016/j.cosrev.2023.100592

[4] Arroyabe, M. F.; Arranz, C. F. A.; Fernandez De Arroyabe, I. & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK, Technology in Society, Vol. 78, 102670, DOI: 10.1016/j.techsoc.2024.102670

[5] ENISA. (2025). ENISA Threat Landscape 2025, European Union Agency for Cybersecurity, ISBN 978-92-9204-723-8, ISSN 2363-3050, DOI: 10.2824/1946374

Working Paper of 37th DAAAM Symposium

[6] Eurostat. (2025). European businesses statistics compilers' manual for ICT usage and e-commerce in enterprises: 2025 survey, Publications Office of the European Union, Luxembourg, ISBN 978-92-68-34786-7, ISSN 2315-0815, DOI: 10.2785/2641073
[7] Eurostat. (2026). Security policy, measures, risks and staff awareness by size class of enterprise (isoc_cisce_ra), statistical dataset, DOI: 10.2908/ISOC_CISCE_RA, Accessed: 2026-08-24.
[8] Eurostat. (2026). Security incidents and consequences by size class of enterprise (isoc_cisce_ic), statistical dataset, DOI: 10.2908/ISOC_CISCE_IC, Accessed: 2026-08-24.
[9] Wooldridge, J. M. (2025). Introductory Econometrics: A Modern Approach, 8th Edition, Cengage, ISBN 978-0-357-90016-1, Boston
[10] Saunders, M. N. K.; Lewis, P. & Thornhill, A. (2023). Research Methods for Business Students, 9th Edition, Pearson, ISBN 978-1-292-40272-7, Harlow
[11] Pejić Bach, M.; Jajić, I. & Kamenjarska, T. (2023). A bibliometric analysis of phishing in the big data era: High focus on algorithms and low focus on people, Procedia Computer Science, Vol. 219, pp. 91-98, ISSN 1877-0509, DOI: 10.1016/j.procs.2023.01.268.

Working Paper of 37th DAAAM Symposium