Reframing Cybersecurity Education through Technical, Organisational, and Regulatory Integration: Google Grant Implementation Case Study at WUT

Krzysztof Ejsmont[1][0000-0003-1516-0878], Jerzy Krawiec[1][0000-0001-5535-1850], Sebastian Zielinski[1][0000-0002-8443-8944], Marek Porzezyński[1][0000-0002-4709-2788], Michal Wisniewski[1][0000-0003-3435-3114], Pawel Gepner[1][0000-0003-0004-1729], and Mieczyslaw Morawski[1][0000-0002-4557-4185]

Warsaw University of Technology, Warsaw, Poland
{krzysztof.ejsmont,jerzy.krawiec,sebastian.zielinski,
marek.porzezynski,michal.wisniewski,pawel.gepner,
mieczyslaw.morawski}@pw.edu.pl

Abstract. Cybersecurity education is increasingly influenced by evolving socio-technical risks and regulatory requirements imposed by the European Union. In particular, the Network and Information Security Directive (NIS2), the Critical Entities Resilience Directive (CER), and the Digital Operational Resilience Act (DORA) require management accountability, incident reporting, resilience testing, and systematic risk management, which cannot be addressed by tool-centred curricula alone. This paper reframes cybersecurity education as an integration of technical, organisational, and regulatory competencies and presents a case study of the Google Cybersecurity Seminars (GCS) programme at the Warsaw University of Technology (WUT). Delivered across three faculties in 2024–2026, the programme combines a 135-hour curriculum with peer-led outreach in schools. In the first project year, 271 students enrolled, 137 completed the full track, and 73 received specialist certificates. A computer-assisted web interview (CAWI) survey conducted in February 2026 (n=40) indicates strong self-reported gains in knowledge, confidence in teaching others, and online behaviour. The case study suggests that regulatory-driven integration can support both professional readiness and community impact.

Keywords: Cybersecurity education · interdisciplinary curriculum · NIS2 · DORA · CER · ISO/IEC 27001 · ISMS · peer-led learning

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

1 Introduction

Cybersecurity (network and information systems security) refers to the resilience of digital systems against threats that compromise confidentiality, integrity, and availability [18]. The rapid growth of cloud services, IoT/IIoT and platform-based work has expanded the attack surface and increased the socio-technical character of incidents. Economic impact estimates illustrate the scale: global cybercrime losses are projected to exceed $10 trillion per year in the mid-2020s and continue rising [1].

In the European Union, this escalation is matched by a regulatory shift from "best-effort" security towards auditable, risk-based resilience. The NIS framework [2] and, more recently, NIS2 [3] extend requirements across sectors and introduce clearer obligations for governance, incident reporting, and security testing. Complementary instruments reinforce these expectations: the Digital Operational Resilience Act (DORA) mandates operational resilience management and testing in the financial sector [16], while the Critical Entities Resilience (CER) directive emphasizes continuity and exercises for essential services [17]. These instruments collectively elevate management accountability, structured risk treatment, supplier assurance, and evidence-based reporting.

This creates an educational challenge. Tool-centred curricula (focused on configuration, scripting, or penetration testing alone) are not sufficient to meet the competency profile implied by EU obligations: graduates must be able to translate regulatory requirements into organisational controls, implement and validate technical safeguards, and communicate evidence to decision-makers and authorities. At the same time, universities face scaling constraints (limited teaching capacity) and a societal need to raise cyber hygiene beyond specialist groups.

This paper reframes cybersecurity education as an integration of three competence domains—*technical*, *organisational*, and *regulatory*—and reports a case study of implementing that approach through the Google Cybersecurity Seminars (GCS) programme at the Warsaw University of Technology (WUT). Our contributions are:

- a concise mapping from EU resilience obligations (NIS2/CER/DORA) to learning outcomes across the three domains;
- an implementation blueprint for an interdisciplinary, 135-hour programme delivered across three faculties, including a scalable peer-led outreach component;
- preliminary evaluation evidence (CAWI survey, n=40) on learning, career intentions, and behavioural change.

The remainder of the paper reviews the state of the art in cybersecurity education and governance-oriented training (Sect. 2), formalises the interdisciplinary technical–organisational–regulatory framing (Sect. 3), details the programme design and delivery model (Sect. 4), describes the case-study evaluation method (Sect. 5), reports outcomes (Sect. 6), and discusses implications and limitations with replication guidance (Sect. 7).

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

2 Related Works

Cybersecurity education research increasingly treats upskilling as a continuous process rather than a one-time qualification, especially in computational science and research-support contexts. Systematic reviews show high variance in outcomes across training methods and emphasise modular, competency-based designs that can be tailored to roles and constraints [4]. Surveys of curriculum activities similarly report that effective programmes combine structured exercises, realistic case studies, and broader curriculum integration, but struggle with the socio-technical nature of security where technical content interacts with organisational routines and human behaviour [5].

A second stream stresses governance and law as first-class educational targets. Socio-technical cyber resilience frameworks argue that risk reduction depends on organisational structures, responsibility allocation, and decision-making processes rather than tools alone [6]. In parallel, board-level cybersecurity governance research highlights the need to teach oversight mechanisms, reporting, and accountability as part of professional readiness [39, 40]. These insights align with EU policy that links resilience to measurable management practices.

Evidence-based awareness programmes aim to change behaviour, not only increase knowledge. Studies grounded in behavioural theory and multi-level evaluation (e.g., Kirkpatrick-style models) show that carefully designed interventions can influence intended behaviour, while measurement beyond short-term feedback remains challenging [8]. University-focused studies consistently find uneven baseline awareness and recommend structured, evaluated interventions rather than ad-hoc sessions [9].

A practical barrier is scale. Active learning strategies in computing education typically improve engagement and learning outcomes [10]. Peer-led instruction can scale delivery, but requires standardised materials, supervision, and quality assurance to avoid uneven outcomes [11]. Finally, hands-on laboratories and cyber ranges are widely considered essential; systematic reviews and experience reports highlight trade-offs between realism, maintenance effort, and learning objectives, with scenario-based labs often providing a practical balance [12–14].

2.1 Regulation- and evidence-oriented training

Recent work increasingly frames cybersecurity education around demonstrable governance practices and evidence generation. Standards-based approaches (e.g., ISO/IEC 27001-style ISMS) provide a pragmatic scaffold that links technical controls to policies, continuous improvement, and audit artefacts [19, 20]. Governance and oversight research similarly argues that graduates should be able to translate technical findings into decision-ready reporting and metrics, rather than treating compliance checklists as a substitute for risk reasoning [39, 41, 42]. In the EU context, DORA further reinforces resilience testing and structured operational risk management as educationally relevant competencies [16, 37].

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

2.2 Security culture and scalable outreach

Security culture models describe resilience as a function of everyday behaviours and people-risk management, implying that education should explicitly target habits and communication [46–48]. For resource-constrained actors (small and medium-sized enterprises (SMEs) and civic organisations), lightweight risk analysis and minimal control baselines can be particularly impactful [45, 49]. Scalable delivery therefore benefits from supervised peer-led instruction [11] and curated e-learning resources that sustain engagement beyond single events [50].

Across these strands, a gap remains: relatively few case studies document how to operationalise *regulatory-driven* integration of technical, organisational and legal competencies in a scalable university setting while also generating community impact. The GCS implementation at WUT is designed to address this gap.

3 Interdisciplinary approach

EU policy explicitly links cybersecurity resilience to education and workforce development. The EU Cybersecurity Strategy for the Digital Decade frames education as a pillar for resilience and highlights a persistent shortage of qualified specialists [15]. NIS2 requires Member States to promote cybersecurity education and training and strengthens expectations for structured risk management, incident handling, and testing [3]. DORA reinforces an "all levels" approach to ICT risk awareness and mandates resilience testing and role-appropriate training [16], while CER emphasises continuity planning and exercises for critical entities [17].

From an educational perspective, these instruments imply an integrated competency model:

1. **Technical competencies** (security engineering and validation): architecture and configuration of secure systems, threat modelling, vulnerability management, penetration testing, and evidence generation via testing and monitoring (e.g., OWASP-aligned web security testing [29] and Adversarial Tactics, Techniques, and Common Knowledge (MITRE ATT&CK)-informed adversary simulation [32]).
2. **Organisational competencies** (governance and risk operations): accountability, roles and segregation of duties, risk treatment planning, business impact analysis (BIA), crisis management, and measurable by key performance indicators (KPIs/KRIs) that connect controls to business objectives [41, 42].
3. **Regulatory competencies** (compliance and accountability): interpretation of obligations (reporting timelines, evidence requirements, outsourcing and supplier assurance, lawful information sharing), including interactions with GDPR/PSD2 and platform regulation (DSA) in operational decision-making [33, 34, 36].

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

Table 1. Examples of translating EU resilience obligations into teachable artefacts and outcomes (based on NIS2 [3], DORA [16] and CER [17]).

Driver	Typical obligation / evidence	Primary competence	Example student artefact (GCS)
NIS2	Risk analysis, policies, control effectiveness assessment	Org + Tech	Risk register; control test plan; evidence report
NIS2	Incident handling and reporting workflow, evidence log	Reg + Org	Incident-report template; decision tree; evidence checklist
DORA	Resilience testing and learning from test outcomes	Tech	Scenario-based test report; EDR/attack-simulation debrief
DORA	Outsourcing responsibility and ICT supplier assurance	Reg + Org	Third-party assurance matrix (contracts, audits, minimum controls)
CER	Continuity preparedness and exercises for essential services	Org	Business impact analysis (BIA) sketch; RTO/RPO targets; tabletop exercise script
GDPR/DSA interplay	Lawful information sharing and online-risk response	Reg	Case analysis: what can be shared, when, and with whom

3.1 From regulatory obligations to teachable competencies

To make the triad actionable in course design, we map representative obligations from NIS2/CER/DORA to the kinds of evidence an organisation must be able to produce, and then to teachable student artefacts. Table 1 summarises this translation layer. The intention is not to provide a legal interpretation, but to show how regulation can be operationalised as curriculum requirements that students can practise end-to-end.

Crucially, the three domains must be taught *as a system*. Regulatory requirements motivate organisational policies and procedures; these, in turn, constrain technical design and define what must be tested and evidenced. Conversely, technical realities (attack paths, control effectiveness) inform risk decisions and compliance prioritisation. Therefore, the learning outcomes of an effective programme should include the ability to: (i) translate requirements into an actionable control set (e.g., ISMS scope, policies, and controls), (ii) implement and validate controls in realistic scenarios, and (iii) communicate findings to both technical and managerial stakeholders in a form suitable for audits and incident reporting.

The GCS programme at WUT operationalises this integration by embedding ISO/IEC 27001-style ISMS thinking into technical laboratories, pairing it with governance and compliance modules, and extending learning through peer-led outreach that reinforces communication and "teach-back" competencies.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

4 A modified cybersecurity teaching program according to the requirements of the Google Cybersecurity Seminars project

Google Cybersecurity Seminars (GCS) is a grant-funded programme (2024–2026) aimed at educating future cybersecurity leaders and, in parallel, improving cyber hygiene in local communities through peer-led school workshops. At WUT, the programme is delivered across three faculties (Administration and Social Sciences, Mechanical and Industrial Engineering, and Management) to ensure interdisciplinary exposure.

4.1 Programme structure and delivery model

Each participant completes a 135-hour learning path (75 hours of structured classes and 60 hours of guided self-study).

At WUT, the contact teaching was embedded into degree programmes by revising five existing course syllabi and creating one new course module ("Cybersecurity 2") in the Faculty of Mechanical and Industrial Engineering. This allowed the programme to scale without adding a standalone semester course while preserving assessment and quality assurance within established study structures.

Table 2 summarises the programme workload and delivery components. The advanced track extends the core path with additional CyberLab seminars and supervised outreach activities. The curriculum is organised into three coordinated blocks—*Technical*, *Legal/Regulatory*, and *Organisational*—and is supported by three enabling components available to all participants:

- **Cybersecurity Laboratory (CyberLab):** a controlled environment for hands-on exercises, adversary simulation, and security monitoring;
- **Cybersecurity Clinic:** seminars, expert sessions, and exposure to current research/practice through visits and conferences;
- **E-learning platform (CyberKlinikaEdu):** modular materials for reinforcement, self-paced learning, and community-facing content.

Completion is formally recognised with a *Cybersecurity Specialist* certificate, and an advanced track requires additional laboratories and community-teaching activities.

Pedagogically, the programme combines active learning (labs and scenario work) with a structured peer-led outreach model. The outreach component is not treated as "extra": it is a deliberate mechanism to (i) scale awareness activities and (ii) improve students' communication, risk framing, and behavioural-change messaging—capabilities shown to be critical for effective security training and peer-led delivery [10, 11].

4.2 Technical block: ISMS-informed engineering and testing

The technical block is anchored in a systemic approach inspired by ISO/IEC 27001 (ISMS requirements) [19] and is complemented by established testing guidance and methodologies (e.g., NIST-style security testing and Open Worldwide

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

Table 2. Workload and delivery components of the GCS programme at WUT. The core workload is 135 hours per participant (75 contact hours + 60 guided self-study).

Component	Hours	Form / examples
Core contact teaching (integrated into revised syllabi)	75	Lectures, exercises and labs across the three blocks (technical, legal/regulatory, organisational)
Technical track (security engineering and testing)	60	20h lectures + 20h exercises (ISMS artefacts) + 20h labs (hardening, OWASP testing, reporting)
Interdisciplinary seminars (regulatory + organisational)	15	Governance, reporting, continuity, compliance-to-control translation
Guided self-study	60	E-learning modules, readings, mini-assignments, reflection tasks
Advanced track (optional)	–	8 CyberLab seminars, (Endpoint detection and response scenarios), school workshops, non-governmental organisation (NGO) manuals

Application Security Project (OWASP) web application testing) [29]. The goal is not only to teach tools, but to connect technical controls to risk treatment decisions and auditable evidence.

Core topics include security models, threat analysis, OS and network security, access control, applied cryptography, secure coding, security measurement, and audit-oriented testing. Practical work is split between:

- **ISMS artefacts (design-thinking exercises):** drafting policies and procedures that are later "executed" in labs (e.g., access control, information transfer, mobile device use, vulnerability management, cryptographic key management, backup and malware protection).
- **Hands-on laboratories:** configuration and verification tasks (permissions and hardening across OS families), IoT/IIoT reconnaissance and asset visibility, certificate inspection and basic public key infrastructure (PKI) validation, steganography demonstrations, OWASP-aligned web application testing [29], and static analysis of small codebases with report writing.

CyberLab provides the infrastructure required for realistic exercises: a dedicated server environment, network devices, and unified threat management/intrusion detection and prevention system (UTM/IDPS)-class equipment. The advanced track adds adversary simulation and detection/response practice using endpoint detection and response (EDR) software [30] and scenario-driven advanced persistent threat (APT) -style techniques mapped to MITRE ATT&CK [32]. This design follows evidence that scenario-based labs provide a strong realism/effort trade-off compared to full cyber ranges [12, 13].

4.3 Legal and regulatory block: from obligations to controls

The regulatory block operationalises the idea that many technical measures are triggered or shaped by legal requirements. For example, multi-factor authentication adoption in parts of industry has been accelerated by sectoral regulation

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

(e.g., PSD2) [33], while GDPR-driven obligations influence both technical safeguards and organisational documentation [34]. Within the programme, students work with a curated set of EU instruments relevant to resilience and online risk: NIS2 [3], DORA [16], CER [17], and the Digital Services Act (DSA) [36]. The emphasis is on *application* rather than memorisation.

Students complete practical tasks such as:

- building a compliance-to-control mapping ("requirements matrix") for a hypothetical organisation, including incident reporting workflows and evidence collection;
- analysing outsourcing/supply-chain responsibility and translating it into third-party assurance requirements (contracts, audits, and minimum control expectations);
- designing information-sharing and escalation procedures that respect data protection and liability constraints.

This block aims to produce graduates who can explain why a control is needed, how it should be evidenced, and what must be reported when incidents occur.

4.4 Organisational block: governance, risk, and resilience operations

The organisational block addresses the management-accountability logic embedded in NIS2/CER/DORA. Students learn to design governance mechanisms (roles, responsibilities, segregation of duties) and connect them to risk operations. Topics include corporate governance for cybersecurity [39], oversight patterns such as the three-lines model [41], and practical metrics (KPIs/KRIs) for reporting [42]. Operational resilience content covers risk assessment, basic business impact analysis, continuity planning concepts recovery time objective/recovery point objective (RTO/RPO), and crisis communication exercises consistent with regulatory expectations for preparedness and stakeholder communication.

4.5 Community outreach and societal impact

A distinctive element of GCS is peer-led outreach: students deliver workshops in primary and secondary schools and develop materials for NGOs. This component supports the broader objective of building cyber hygiene beyond specialist groups and reinforces students' ability to communicate risks and protective behaviours clearly. The programme design deliberately uses supervised, shared materials and structured sessions to maintain quality, in line with evidence on the conditions under which peer-led models succeed [11].

5 Research design and evaluation method

We report the WUT implementation as a descriptive case study focused on feasibility and early outcome signals. Evidence combines administrative programme

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

data (enrolment and completion) with an exploratory CAWI survey [51] conducted between February 12 and 18, 2026 (MS Forms). Responses were obtained from 40 participants (31 students and 9 teachers). Accordingly, the survey is interpreted as an exploratory programme-level signal rather than a homogeneous student-only outcome measure. The questionnaire contained 30 items covering respondent profile, pre/post perceptions of cybersecurity, and perceived social impact, with a small number of open-ended questions on implemented practices and perceived value. Results are reported descriptively (proportions) and complemented with thematic highlights from open responses. Participation was voluntary and anonymous; Section 7 discusses threats to validity and next evaluation steps.

6 Results

WUT students participated in the GCS programme and submitted the required declarations of participation. In the first project year, 137 students completed the educational track in accordance with Google requirements. In addition, 73 students completed an advanced track: eight CyberLab seminars (EDR/attack simulation), participation in workshops delivered in schools, and preparation of exercise manuals for NGOs. After meeting these requirements, 73 students received *Cybersecurity Specialist* certificates.

We conducted a preliminary, exploratory evaluation between February 12 and 18, 2026 ($n = 40$) using a CAWI questionnaire [51] (MS Forms) combining closed- and open-ended items. Respondents included 31 students (77.5%) and 9 teachers (22.5%). Baseline self-assessed knowledge varied (mean 2.8/5), with teachers reporting higher initial levels.

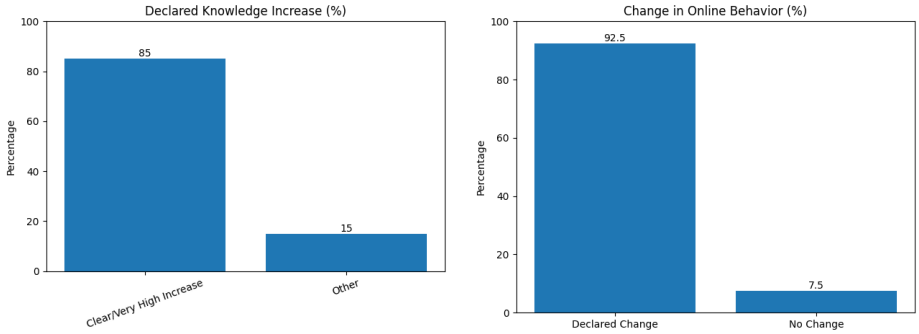
The survey also captured perceived training quality and demand for continued learning. A large majority (82.5%) expressed a need for further cybersecurity education. Teaching quality indicators were positive: 87.5% rated the content as useful or extremely useful, 76.9% rated instructor preparation as positive, and 90% judged the difficulty level as appropriate. Engagement was also encouraging, with 62.5% describing the classes as clearly engaging.

Key quantitative signals are summarised below and illustrated in Fig. 1 and Fig. 2.

After the course, 85% reported a "clear" or "very high" increase in knowledge, 97.4% reported increased confidence in teaching others, and 61.5% reported a clear/very high increase in readiness to use skills professionally. A strong behavioural signal was observed: 92.5% declared changes in online behaviour (including 20% "radical" change). Figure 1 summarises the learning and behavioural outcomes.

The course also influenced career intentions. Before participation, only one respondent reported applying for positions requiring cyber skills, whereas after the course 57.5% declared an intention to apply. This shift should be interpreted cautiously, as it reflects self-reported intentions rather than observed career outcomes. In the subgroup planning to apply ($n = 23$), 78.3% rated the course

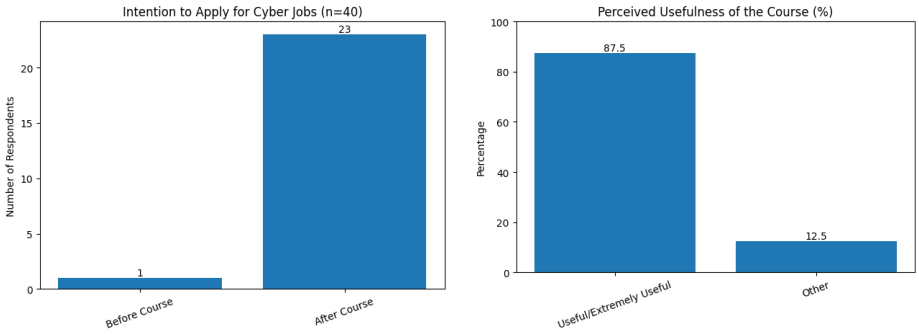
ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33



(a) Declared knowledge increase. **(b)** Declared change in online behavior.

Fig. 1. Self-reported learning and behavioral outcomes after course completion ($n = 40$).

as clearly/very highly influential. Perceived usefulness was high: 87.5% found the content useful or extremely useful. Additionally, 10% declared an intention to start a business requiring cybersecurity competencies; respondents in this subgroup consistently rated the programme as a significant or very highly significant influence on that decision. Figure 2 presents the career-intention shift and perceived usefulness.



(a) Intention to apply for cyber jobs. **(b)** Perceived usefulness of the course.

Fig. 2. Career intention and perceived usefulness outcomes after the course ($n = 40$).

Open-ended responses most often mentioned immediate practice changes (password hygiene, caution toward suspicious messages, and increased use of multi-factor authentication). Participants also highlighted the value of real-life examples and the combination of technical, organisational and regulatory content.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

7 Discussion, limitations, and replication guidance

7.1 Interpretation and educational implications

The results support the central design claim of this paper: treating regulation as a competency scaffold can improve the coherence of cybersecurity education. Rather than presenting NIS2/CER/DORA as external constraints, the programme turns them into prompts for concrete artefacts (policies, test evidence, reporting workflows) that students can build and critique. Embedding ISMS-informed documentation into technical laboratories helps students connect "what a control does" with "how an organisation proves it works"—a linkage frequently missing from tool-first curricula [19, 20, 41, 42]. The strong increase in confidence to teach others (97.4%) suggests that the peer-led outreach component acts as a deliberate "teach-back" mechanism that reinforces understanding and communication, aligning with evidence on supervised peer-led learning [11].

A second implication is the explicit integration of governance and resilience operations. NIS2 and DORA elevate management accountability and testing, which implies that graduates need to operate across technical and managerial interfaces. By teaching oversight patterns (e.g., three lines) [41] and boardroom expectations [39, 40], the programme prepares students to translate technical findings into risk and compliance language that decision-makers can act on.

7.2 Sustainability and scale

Two choices supported scale: integrating teaching into existing syllabi (reducing standalone staffing pressure) and sharing enabling infrastructure (CyberLab, Clinic, and e-learning) across cohorts. The community-facing strand aligns with the view that security culture and habit formation require repeated engagement rather than one-off awareness events [46, 47]. Curated platform materials also support continuity and reuse [50].

7.3 Threats to validity

The present evaluation has several limitations. *Construct validity* is constrained because outcomes are self-reported and may reflect social desirability or short-term optimism. *Internal validity* is limited by the lack of a control group and potential self-selection (motivated participants may be over-represented). *External validity* is constrained because the case is specific to WUT, its faculty mix, and its infrastructure. Finally, *conclusion validity* is limited by the small sample size ($n = 40$) and descriptive analysis.

7.4 Next evaluation steps

To strengthen evidence, future work will (i) add objective skills assessments (practical lab exams and rubric-based artefact grading), (ii) include pre/post

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

measures and longitudinal follow-up, and (iii) incorporate scenario-based incident response exercises with structured debriefs. A comparative evaluation across cohorts with different proportions of technical versus governance/regulatory content would help isolate which elements drive behavioural change and professional readiness.

7.5 Replication guidance

For replication, a practical minimum is to (i) pick a small set of regulatory obligations (reporting, testing, continuity), (ii) require students to produce both governance artefacts and technical evidence, and (iii) use supervised peer-led "teach-back" to scale outreach and strengthen communication [3, 11, 16, 17, 20].

8 Summary

The GCS case study at WUT suggests that EU "resilience-by-design" regulation can be used as a constructive curriculum driver rather than an external compliance constraint. By aligning learning outcomes with NIS2/CER/DORA expectations, the programme trains students to connect (i) technical safeguards and testing evidence, (ii) organisational governance and risk operations, and (iii) regulatory obligations and reporting practices. The peer-led outreach component further extends impact by translating specialist knowledge into community-facing cyber hygiene interventions while strengthening students' ability to communicate risk and motivate safer behaviour.

The preliminary evaluation indicates strong self-reported gains in knowledge, teaching confidence, and behavioural change, alongside increased intention to pursue cyber-related roles. These findings are encouraging but should be interpreted with caution. The current evidence is based on a small sample ($n = 40$), self-reported measures, and a short post-intervention window. Future work will therefore focus on longitudinal tracking, adding objective measures (skills assessments, artefact quality, incident-response exercises), and comparing cohorts exposed to different mixes of technical, organisational, and regulatory content.

Overall, the programme provides an actionable blueprint for universities seeking to modernise cybersecurity education for computational science: treat regulation as a competency scaffold, embed ISMS thinking into laboratories, teach governance as an operational discipline, and scale societal impact through supervised peer-led delivery.

References

1. Braue, D.: Cybercrime To Cost The World $12.2 Trillion Annually By 2031. Cybercrime Magazine. (2025).
2. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, (2016).

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

3. Directive 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2)., (2022).
4. Prümmer, J., Van Steen, T., Van Den Berg, B.: A systematic review of current cybersecurity training methods. Computers & Security. 136, 103585 (2024). https://doi.org/10.1016/j.cose.2023.103585.
5. Ismail, M., Madathil, N.T., Alalawi, M., Alrabaee, S., Al Bataineh, M., Melhem, S., Mouheb, D.: Cybersecurity activities for education and curriculum design: A survey. Computers in Human Behavior Reports. 16, 100501 (2024). https://doi.org/10.1016/j.chbr.2024.100501.
6. Christine, D.I., Thinyane, M.: Socio-technical Cyber Resilience: A Systematic Review of Cyber Resilience Management Frameworks. In: Marx Gómez, J. and Lorini, M.R. (eds.) Digital Transformation for Sustainability. pp. 573–597. Springer International Publishing, Cham (2022). https://doi.org/10.1016/j.pdisas.2022.100244.
7. Wells, E.M., Boden, M., Tseytlin, I., Linkov, I.: Modeling critical infrastructure resilience under compounding threats: A systematic literature review. Progress in Disaster Science. 15, 100244 (2022). https://doi.org/10.1016/j.pdisas.2022.100244.
8. Khan, N.F., Ikram, N., Murtaza, H., Javed, M.: Evaluating protection motivation based cybersecurity awareness training on Kirkpatrick's Model. Computers & Security. 125, 103049 (2023). https://doi.org/10.1016/j.cose.2022.103049.
9. Adeshola, I., Oluwajana, D.I.: Assessing cybersecurity awareness among university students: implications for educational interventions. J. Comput. Educ. 12, 1283–1305 (2025). https://doi.org/10.1007/s40692-024-00346-7.
10. Córdova-Esparza, D.-M., Romero-González, J.-A., Córdova-Esparza, K.-E., Terven, J., López-Martínez, R.-E.: Active Learning Strategies in Computer Science Education: A Systematic Review. MTI. 8, 50 (2024). https://doi.org/10.3390/mti8060050.
11. Servin, C., Pagel, M., Webb, E.: An Authentic Peer-Led Team Learning Program for Community Colleges: A Recruitment, Retention, and Completion Instrument for Face-to-Face and Online Modality. In: Proceedings of the 54th ACM Technical Symposium on Computer Science Education V. 1. pp. 736–742. ACM, Toronto ON Canada (2023). https://doi.org/10.1145/3545945.3569851.
12. Stamatopoulos, D., Katsantonis, M., Fouliras, P., Mavridis, I.: Exploring the Architectural Composition of Cyber Ranges: A Systematic Review. Future Internet. 16, 231 (2024). https://doi.org/10.3390/fi16070231.
13. Alrabaee, S., Al-Kfairy, M., Barka, E.: Efforts and Suggestions for Improving Cybersecurity Education. In: 2022 IEEE Global Engineering Education Conference (EDUCON). pp. 1161–1168. IEEE, Tunis, Tunisia (2022). https://doi.org/10.1109/EDUCON52537.2022.9766653.
14. Lazarov, W., Schafeitel-Tähtinen, T., Squillace, J., Martinasek, Z., Coufalikova, A., Helenius, M., Gallus, P., Fujdiak, R.: Lessons Learned from Using Cyber Range to Teach Cybersecurity at Different Levels of Education. Tech Know Learn. (2025). https://doi.org/10.1007/s10758-025-09840-y.
15. Joint Communication to the European Parliament and the Council entitled The EU's Cybersecurity Strategy for the Digital Decade. (2020).
16. Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector. (2022).
17. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. (2022).

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

18. ISO/IEC 27000:2018 Information technology – Security techniques – Information security management systems – Overview and vocabulary.
19. ISO/IEC 27002:2022/Amd1:2024 Information technology – Security techniques – Code of practice for information security controls
20. ISO/IEC 27001:2022/Amd1:2024 Information technology – Security techniques – Information security management systems – Requirements.
21. ISO/IEC 27032:2023 Cybersecurity – Guidelines for Internet security.
22. ISO/IEC 27011:2024 Information technology – Security techniques – Code of practice for Information security controls based on ISO/IEC 27002 for telecommunications organizations.
23. ISO/IEC 27019:2024 Information technology – Security techniques – Information security controls for the energy utility industry.
24. ISO/IEC 27013:2021/Amd1:2024 Information technology – Security techniques – Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1.
25. ISO/IEC 27014:2020 Information technology – Security techniques – Governance of information security.
26. ISO/IEC 27021:2017/Amd1;2021 Information technology – Security techniques – Competence requirements for information security management systems professionals.
27. ISO/IEC 27018:2025 Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.
28. ISO/IEC 27031:2025 Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity.
29. OWASP Top 10 – 2025 Globally recognized by developers as the first step towards more secure coding. (2025).
30. ESET, Endpoint detection & response. (2026).
31. FORTINET, Advanced Persistent Threat: The Silent, Long-Term Cyberattack.
32. MITRE ATT&CK, Enterprise Techniques.
33. Directive 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (PSD2).
34. Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (GDPR).
35. Proposal for a Regulation of the European Parliament and the Council on the European Union Agency for Cybersecurity (ENISA), the European cybersecurity certification framework, and ICT supply chain security and repealing Regulation (EU) 2019/881 (The Cybersecurity Act 2), Strasbourg, 20.1.2026, COM(2026) 11 final, 2026/0011 (COD).
36. Digital Services Act.
37. Buttigieg, C.P., Zimmermann, B.B.: The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. ERA Forum. 25, 11–28 (2024). https://doi.org/10.1007/s12027-024-00793-w.
38. Catal, C., Ozcan, A., Donmez, E., Kasif, A.: Analysis of cyber security knowledge gaps based on cyber security body of knowledge. Educ Inf Technol. 28, 1809–1831 (2023). https://doi.org/10.1007/s10639-022-11261-8.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33

39. Gale, M., Bongiovanni, I., Slapnicar, S.: Governing cybersecurity from the boardroom: Challenges, drivers, and ways ahead. Computers & Security. 121, 102840 (2022). https://doi.org/10.1016/j.cose.2022.102840.
40. Galle, A., Vletter-van Dort, H.: From cybersecurity to cyber resilience in the board room: key steps for supervisory board members and non-executives. Int. Cybersecur. Law Rev. 6, 221–237 (2025). https://doi.org/10.1365/s43439-025-00151-7.
41. Valkenburg, B., Bongiovanni, I.: Unravelling the three lines model in cybersecurity: a systematic literature review. Computers & Security. 139, 103708 (2024). https://doi.org/10.1016/j.cose.2024.103708.
42. Slapničar, S., Axelsen, M., Eulerich, M.: Cyber risk management: an illusion of a risk-based approach. J Manag Control. (2025). https://doi.org/10.1007/s00187-025-00401-z.
43. Kamil, Y., Lund, S., Islam, M.S.: Information security objectives and the output legitimacy of ISO/IEC 27001: stakeholders' perspective on expectations in private organizations in Sweden. Inf Syst E-Bus Manage. 21, 699–722 (2023). https://doi.org/10.1007/s10257-023-00646-y.
44. Rezaei Soufi, H., Torabi, S.A., Sahebjamnia, N.: Developing a novel quantitative framework for business continuity planning. International Journal of Production Research. 57, 779–800 (2019). https://doi.org/10.1080/00207543.2018.1483586.
45. Pawar, S., Palivela, Dr.H.: LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights. 2, 100080 (2022). https://doi.org/10.1016/j.jjimei.2022.100080.
46. Walton, H.: SECURITY CULTURE: a how-to guide for improving security culture and dealing with people risk... in your organisation. ROUTLEDGE, S.l. (2024).
47. Huang, K., Pearlson, K.: For What Technology Can't Fix: Building a Model of Organizational Cybersecurity Culture. MIT Sloan School of Management (2019).
48. Aksoy, C.: Buiding a Cyber Security Cuture for Resilient Organizations against Cyber Attacks. İşletme Ekonomi ve Yönetim Araştırmaları Dergis. 7, 96–110 (2024). https://doi.org/10.33416/baybem.13212345.
49. Chaudhary, S., Gkioulos, V., Katsikas, S.: A quest for research and knowledge gaps in cybersecurity awareness for small and medium-sized enterprises. Computer Science Review. 50, 100592 (2023). https://doi.org/10.1016/j.cosrev.2023.100592.
50. Morawski, M., Jędrzejczyk, W., Jagoda, A. eds: Cyfryzacja zarządzania zasobami ludzkimi. Polskie Wydawnictwo Ekonomiczne, Warszawa (2024).
51. Manfreda, K.L., Batagelj, Z., Vehovar, V.: Design of Web Survey Questionnaires: Three Basic Experiments. Journal of Computer-Mediated Communication. 7, 0–0 (2006). https://doi.org/10.1111/j.1083-6101.2002.tb00149.x.

ICCS Camera Ready Version 2026
To cite this paper please use the final published version:
DOI: 10.1007/978-3-032-29918-5_33