EPiC Series in Computing

Volume 109, 2026, Pages 61–69

Proceedings of EUNIS 2026 Annual Congress

Cybersecurity in European Higher Education: Insights from an Exploratory EUNIS Survey

Harald Gilch[1], Maren Lübcke[1] and Mathias Stein[1]
[1] HIS-Institute of Higher Education Development (HIS-HE), Germany
gilch@his-he.de, luebcke@his-he.de, stein@his-he.de

Abstract

This paper presents the results of an exploratory survey conducted within the EUNIS community to better understand the state of IT security in European higher education institutions. Building on previous comparative studies in Germany, Austria, and Switzerland, the aim was to gain initial insights into current practices, organizational structures, external support mechanisms, and emerging challenges. A total of 19 institutions from ten European countries participated in the survey, providing qualitative and structural information that – despite the modest response rate – offers valuable indications of sector-wide trends. The findings show that universities face a complex constellation of challenges, including increasing threat dynamics, decentralized IT landscapes, limited resources, and growing regulatory requirements such as NIS2. At the same time, institutions report a wide range of preventive and reactive measures, advancing ISMS implementation, and improving cooperation within national and sector-specific security networks. The paper concludes with an assessment of limitations and outlines options for a more comprehensive European-wide study.

1 Introduction

Cybersecurity is a principal component of infrastructure and data protection in today's digital world. This topic is particularly important for universities in Europe, as they manage a large amount of sensitive information that must be protected against unauthorised access, theft, and damage. Universities are not only places of education, but also centres of research and innovation, making them attractive targets for cyber-attacks. In 2024, the HIS Institute for Higher Education Development (HIS-HE) presented recommendations for responding to cyberattacks at universities at the EUNIS conference in Athens (Gilch et al., 2024a). These recommendations were developed based on the experiences of German universities that had been victims of cyber-attacks and, due to the great interest they received, were published in English with the support of EUNIS (Gilch et al., 2024b). In 2025, HIS-HE highlighted how the German federal states, which are responsible for universities, are responding to these challenges (Gilch et. al., 2025). The strategies and approaches of the state governments to support universities

L. Desnos, C. Diaz, J. Mincer-Daszkiewicz, L. Merakos, R. Vogl, S. McLellan and U. Lucke (eds.), EUNIS 2026 (EPiC Series in Computing, vol. 109), pp. 61–69

range from ‘extensive autonomy and self-responsibility for IT and cyber security’ (autonomy strategy) to a ‘state-wide strategy and joint financial and organisational support’ (network strategy). The 2025 study was very well received and led to considerations of conducting such a comparative analysis at European level with the help of the EUNIS community.

This idea gave rise to a short explorative survey, the results of which are presented in this paper. The online survey was launched on December 18, 2025, and was open until January 30, 2026.

2 Survey Structure and Response

The survey contains 16 open and closed questions within the following 4 topic areas: current IT security practices and precautions, organisational structures and governance, external support networks and collaborations, key challenges, and priorities for the coming years.

Response rate was 19 completely filled questionnaires 4 from Finland, 3 from Italy and Germany, and 1 from Belgium, Denmark, Greece, Luxembourg, Norway, and Spain each. 12 questionnaires are from Universities while 2 are from Universities of Applied Science. 14 are public founded (state government) institutions. 3 have not provided further details about their specifications. The size of the university is evenly distributed, ranging from small universities to large ones (see Figure 1).

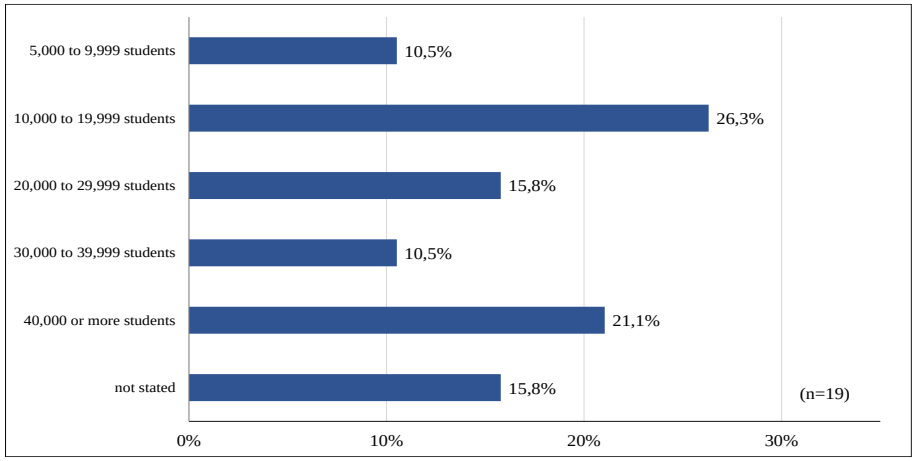

Figure 1: Distribution of participating universities by number of students

As the response rate to the survey is relatively low, the results are partly compared with results of a survey conducted by HIS-HE at German, Austrian and Swiss universities on the status of digitalisation in 2025, which asked similar questions and was also presented in part at the EUNIS Congress 2025 in Dublin (Gilch & Wannemacher, 2025). At that survey, response rates of 32.2% (n=138) in Germany and 33.3% (n=26) in Austria were achieved, compared to only 7.9% (n=11) in Switzerland, providing a solid data base at least for Germany.

3 Results

3.1 Current IT Security practices and precautions

The majority of institutions (58.8%) state that they have not been affected by cyber-attacks. Meanwhile, 41.2% have already experienced an attack, albeit with varying degrees of damage. The figures (EUNIS-Survey) correspond to the data collected for Germany in 2025 (Survey-Germany), as shown in the Figure 2. In contrast, the majority of the Austrian universities surveyed reported that they had not experienced any cyber-attacks with known or unknown damage. Specifically, 80.8% of them have not recorded any major attacks to date.

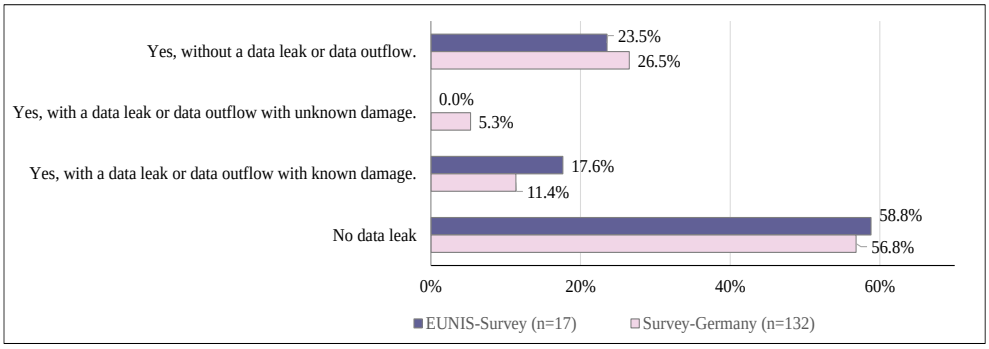

Figure 2: "Has your institution been or is your institution affected by a cyber-attack?"

Most participants in the EUNIS survey (57.1%) stated that the effects of an attack lasted only a few hours. This indicates an efficient response capability, but the fact that 28.6% of institutions struggled with effects lasting months shows that long-term damage is possible. The feedback from German universities is even clearer, as they appear to deal with the damage for much longer, as Figure 3 shows.

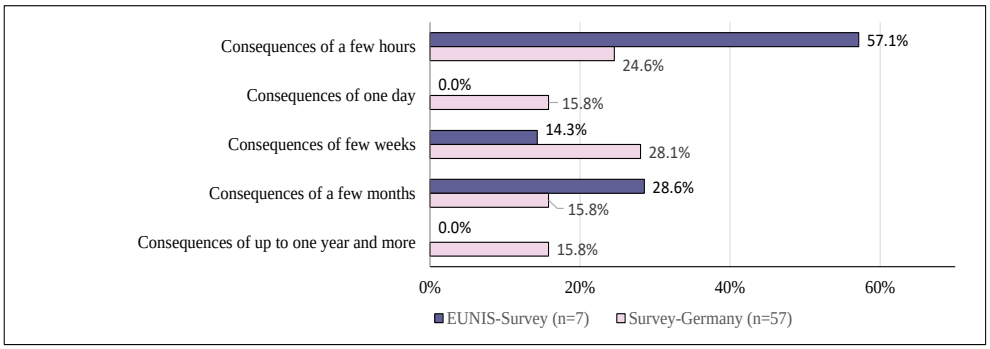

Figure 3: "How long did the effects and restrictions of the attack last?"

If we distinguish between prevention, detection, and response to a cyber-attack as phases (see Figure 4), it becomes apparent that responding EUNIS members are most confident in their own ability to prevent cyber-attacks, and less confident in their ability to detect and respond to them. The greatest uncertainty lies in preparing for the response.

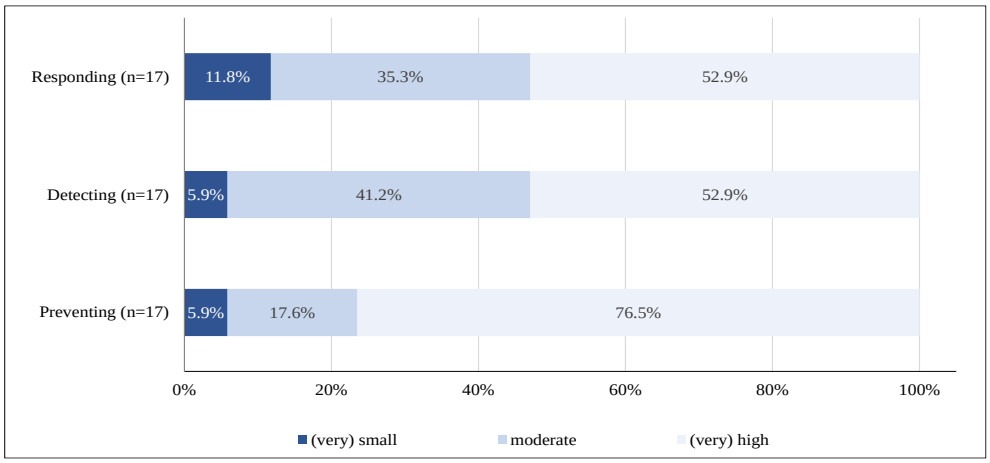

Figure 4: "How well prepared do you think your institution is in terms of preventing, detecting and responding to cyber-attacks?"

As a result of a cyber-attack, the following measures in particular are being developed:

- Introduction of business continuity management
- Defining emergency measures and crisis management measures
- Integrating IT security management into the general crisis management of our university

The following measures in particular have been taken preventively, i.e. before a successful cyber-attack:

- Introduction of information security management
- Introduction of cybersecurity asset management
- Definition of security guidelines and measures
- Awareness training for employees
- Establishment of new structures to monitor our systems for anomalies
- Reassignment of responsibility for IT security, e.g. appointment of a Chief Information Security Officer
- Implementation of a university-wide risk analysis and review of the security standard
- Expansion of technical security/detection measures

Awareness measures for students are mentioned significantly less frequently than the measures listed above, both in terms of prevention and response to a cyber-attack.

On the technical side, most organisations have implemented a wide range of cybersecurity measures. The most common cybersecurity measures are firewalls, endpoint detection (EDR), centralised log analysis (SIEM), and multi-factor authentication. At the same time, the importance of strategic approaches such as the defence-in-depth approach with network segmentation, vulnerability management and increasing organisational anchoring via ISMS/ISO27001 is becoming clear.

3.2 Organisational structures, governance, and future challenges

The implementation of information security management systems and IT service management (ITSM) is the most advanced. Here, over 50% of respondents say they have already fully implemented both approaches. In contrast, the business continuity management system (BCMS) has only been fully implemented by a good quarter of respondents.

The majority of institutions (82.4%) prefer a hybrid solution for hosting their IT infrastructure as a mixture of on-premises and cloud services, which enables flexibility and scalability. Notably, neither a fully cloud-based approach nor the use of shared data centres with other institutions was reported by any respondent.

When asked about the biggest challenges, the following areas were mentioned:

- In the **area of IT security**, phishing emails are becoming increasingly targeted and effective due to the use of artificial intelligence. At the same time, vulnerability management remains a continuous challenge, as exploitation cycles are becoming significantly shorter and newly discovered weaknesses are leveraged more rapidly by threat actors. In parallel, the growing number of IT services further expands the institutional attack surface and increases overall exposure to cyber risks.
- **IT infrastructure** is characterized by a highly distributed and heterogeneous academic and administrative landscape, resulting in limited standardization and increasing complexity in hybrid IT environments. In some cases, research departments or academic schools maintain their own independent IT infrastructures with unclear or varying security levels. The continued operation of legacy systems further complicates efforts to maintain a consistent and modern security posture.
- From a **user and organizational perspective**, the human factor represents a core cybersecurity risk. Collaboration with multiple internal and external stakeholders increases the complexity of third-party risk management. Additional internal challenges include high staff turnover, heterogeneous IT teams with differing levels of maturity, and IT departments that are often understaffed. Furthermore, limited engagement or resistance among faculty members can hinder the consistent implementation of security measures.
- From **a governance and legal standpoint**, ensuring consistent information security management across a complex and decentralized academic environment requires a shared understanding of risks, scope, and responsibilities. Institutions must balance the traditional openness required for education and research with growing regulatory and threat-driven security requirements. Regulatory frameworks such as NIS2 must be systematically implemented and monitored. At the same time, strong reliance on proprietary software from major IT providers such as Microsoft and Google necessitates robust governance structures, effective supplier management, and continuous risk assessment due to the increasing dependency on external digital services and cloud-based solutions.

Respondents were also asked about factors that support or hinder IT security. On the **hindering side**, a general lack of resources remains a central challenge.

- Limited budgets and insufficient human capital restrict the ability to implement and sustain adequate security measures. In particular, the shortage of specialised cybersecurity staff constrains operational capacity and slows down the development of more mature security processes.
- Organisational complexity further complicates IT security efforts. Universities typically operate within highly decentralised and heterogeneous IT environments, making standardisation and

harmonisation difficult. Many research departments or academic schools maintain their own independent IT infrastructures, and as mentioned before, sometimes with unclear or varying levels of security. This decentralised structure increases management complexity and limits the institution's ability to enforce consistent security policies. Additionally, the uncontrolled use of consumer cloud services—both traditional platforms and AI-based tools—introduces further risks, particularly when such services are adopted without central oversight or risk assessment.

- Cultural and behavioural factors also play a significant role. Non-IT staff often lack sufficient cybersecurity awareness and skills, and the human factor remains a persistent vulnerability. Interaction with academic staff can be particularly challenging, as their need for openness, flexibility, and rapid information exchange does not always align easily with regulatory and security requirements. In some cases, attitudes toward cybersecurity or established ways of working may slow down the adoption of protective measures. Furthermore, competing institutional priorities and rapid digital transformation initiatives can hinder the consistent and long-term implementation of security controls across the organisation.

At the same time, several **promoting factors** strengthen IT security in the academic context.

- Visible and vocal support from university leadership, including the rectorate, significantly enhances the legitimacy and prioritisation of cybersecurity initiatives. Growing management awareness and the allocation of additional resources to information security demonstrate strategic commitment. Structured IT security governance, supported by established frameworks and regulatory drivers such as the NIS2 Directive, provides a clearer compliance and risk management baseline.
- Institutions that have implemented a mature Information Security Management System (ISMS), integrated risk management, change management, and incident handling processes, and developed strong IT service management capabilities are better positioned to manage cyber risks systematically. Active cooperation with national and sector-specific security networks further strengthens resilience through information sharing and coordinated response capabilities.
- Interestingly, the heterogeneous IT landscape, while challenging from a governance perspective, can also provide a degree of intrinsic resilience: decentralised structures may limit lateral movement during cyberattacks and reduce the potential blast radius of security incidents. Finally, the enthusiasm and commitment of central IT staff often function as a critical enabling factor, driving initiatives forward despite structural and resource-related constraints.

4 Summary and further actions

4.1 Summary

The results of this study are subject to several limitations. Most notably, the response rate was comparatively low. This restricts the generalizability of the findings and may introduce non-response bias. However, despite this limitation, the results remain analytically valuable. The responses to the same questions are comparable to those in the German survey, which allows for cautious cross-reference and contextual interpretation. Moreover, the data provide important qualitative and structural insights into perceived challenges, barriers, and enabling factors within the field. Two qualitative follow-up interviews – conducted with representatives of a German university of applied sciences and a Greek university – further enrich the findings by providing contextual depth on governance structures, national support frameworks, and the practical realities of cybersecurity management. In this respect,

the findings contribute meaningful exploratory evidence and highlight relevant dimensions for future, more comprehensive investigations.

Overall, IT security in higher education is shaped by a dynamic interplay between resource limitations, decentralised complexity, and cultural factors on the one hand, and leadership commitment, governance maturity, and collaborative networks on the other.

41.1% of respondents reported cyberattacks with varying degrees of damage, which shows how highly relevant this issue is. The survey results highlight that IT security in European higher education institutions is shaped by a combination of technical, organisational, and human-centric factors. While respondents report a broad spectrum of preventive measures—ranging from firewalls and multi-factor authentication to ISMS implementation—several challenges remain prominent across institutions. These include increasingly sophisticated cyberattacks, often supported by AI-driven methods; heterogeneous and decentralised IT environments that hinder standardisation; and the continued operation of legacy systems. Organisational barriers such as limited staffing, and varying levels of cybersecurity awareness further impede a consistent security posture.

At the governance level, universities must balance openness in research and teaching with rising regulatory and security requirements. Frameworks such as NIS2 demand clearer risk management structures, more robust supplier governance, and coordinated approaches across decentralised organisational units. Despite these obstacles, several factors strengthen institutional resilience: committed leadership, maturing security management processes, national collaboration networks, and the dedication of central IT staff.

In their recent blog post, Küfer & Thorsen (2026) pointed out similar challenges faced by universities in protecting themselves against cyber-attacks. They noted that the need to provide systems that are as open as possible for scientific exchange and collaboration necessarily increases vulnerability to cyber-attacks. However, the goal cannot be to completely isolate all IT systems, which means that universities must also focus strongly on organisational measures, clear management structures, trained personnel and a culture of transparency and continuous improvement to prevent cyber-attacks. Last but not least, collaboration between universities within national networks – ideally with government support such as that provided to Norwegian universities by the Directorate for Higher Education and Skills (Sidselrud, 2025) – and at the international level – for example, through the EUNIS Information Security Special Interest Group (InfoSec SIG) – are other key elements of prevention. However, due to the small number of participants in this survey, it is not yet possible to quantify such collaboration at this stage.

4.2 Further Actions

Following the survey, HIS-HE conducted follow-up interviews with representatives of two participating universities – one from a university of applied sciences in Germany and one from a university in Greece. While the original plan envisaged a larger number of interviews covering Northern, Central, and Southern Europe, only two institutions took part. Despite the small number, the interviews provide valuable qualitative insights that complement and deepen the survey findings.

Both interviews confirm the survey's core findings regarding governance structures and organisational challenges. The German interviewee described a security setup that reflects the survey's picture of maturing governance: an ISMS in place, structured incident reporting via a CERT working group, and active participation in the EUNIS Information Security Special Interest Group. The Greek interviewee reported a comparable structural trajectory: central ISO standards including business continuity management have been established over time, though individual departments continue to operate their own infrastructures – a situation described pragmatically as "live and let live."

On external support and collaboration, both interviews point to the importance of national and international networks, while also revealing notable differences in their maturity. The use of AI-based

tools for threat detection – including automated blocking of anomalous user behaviour and tools such as Microsoft Defender – was mentioned as an emerging but still limited capability.

In Germany, the Federal Office for Information Security (BSI) provides guidelines and standards, though the federal structure means that support for universities varies considerably across states (cf. Stein et al., 2025). The extent to which larger cyberattacks—which have led to extended shutdowns of entire IT systems—have actually already occurred at universities in the federal state also appears to play a role here. This appears to be the case in Greece as well, as there has been only one major documented case of a cyberattack there to date—albeit at a smaller university (Hellenic Open University in October 2024[*]). This may explain why, in Greece, there appear to be few cross-university support structures for the prevention of cyberattacks, as is also the case in German federal states with similar circumstances. This assessment, which certainly warrants further discussion, must not, however, be misunderstood to mean that a serious cyberattack should always be awaited as the trigger for cross-university government support activities. Rather, it is essential to use the time gained so far to expand measures supporting universities in the prevention and defense against cyberattacks now, so that an escalated situation—such as the one that has already occurred at many institutions—does not arise initially.

Together, the two interviews illustrate how similar structural challenges – decentralised IT, resource constraints, dependency on major software vendors, and the tension between openness and security – manifest differently depending on national context, regulatory environment, and available support structures. These findings reinforce the case for a broader European comparative study. The availability of survey data from Germany and Austria, each with comparatively robust response rates, offers a strong methodological foundation for such an endeavour. The Digi 2.0 survey instrument of HIS-HE could provide a solid starting point for the development of a standardised data collection framework across multiple countries, enabling more robust cross-national comparisons and contributing to a deeper understanding of structural patterns, risk factors, and resilience mechanisms in European higher education.

References

Gilch, H., Lübcke, M. & Stein, M. (2025): Cybersecurity in Higher Education: Different Approaches in the German Federal States to Support Universities in Defending Against Cyber-Attacks. Proceedings of European University Information Systems Congress, vol 107 2025, pages 156–261. https://easychair.org/publications/paper/HHvx/open

Gilch, H. & Wannemacher, K. (2025): Development and status of digitalization in universities: Germany | Austria | Switzerland. Presentation at the EUNIS Congress 2025, Belfast, UK. June 6, 2025: https://drive.google.com/file/d/1sthiNQbxz1xOtOBTzvLXxEsD20KHW4QB/view

Gilch, H., Lübcke, M. & Stein, M. (2024a): More than technology: crisis management after cyber-attacks - recommendations for higher education management. Presentation at the EUNIS Congress 2024, Athens, Greece. June 6, 2024: https://drive.google.com/file/d/1Bfqdzp_GEsE5SjquTodf8ashNJLcGdBT/view

Gilch, H., Lübcke, M. & Stein, M. (2024b): Crisis management after cyber-attacks - Recommended Actions: https://eunis.org/wp-content/uploads/2025/01/2024_HIS-HE_Crisis-management-after-cyber-attacks-1.pdf

[*] https://security.geant.org/hellenic-open-university-hit-by-cyberattack-813-gb-of-personal-data-leaked-on-dark-web/

Küfer, T. and Thorsen, A. (2026): Strengthening Cyber Resilience in Higher Education Through Collaboration. https://eunis.org/blog/article/strengthening-cyber-resilience-in-higher-education-through-collaboration/

Sidselrud, A. (2025): Need to reduce risk in information security? Asset management is your secret ingredient. Presentation at the EUNIS Congress 2025, Belfast, UK. June 6, 2025: https://drive.google.com/file/d/19sMvj3DR9izzbtZ0otAd2DdxOUPmGD1-/view

Stein, M., Lübcke, M. & Gilch, H. (2025): Cybersicherheit an Hochschulen: Föderale Ansätze und (gemeinsame) Wege. HIS-HE:Forum 3|2025. HIS-Institut für Hochschulentwicklung, Hannover. https://his-he.de/publikation/cybersicherheit-an-hochschulen-foederale-ansaetze-und-gemeinsame-wege/

5 Biographies of Authors

Dr. Harald Gilch is senior consultant and project manager in the Higher Education Management department of the HIS-Institute of Higher Education Development (HIS-HE) in Hannover. He supports universities in the areas of university organization and management, IT services and benchmarking and has a focus on the digitalization of university administration.
gilch@his-he.de , phone: +49 511 169929-36.
HIS-Institut für Hochschulentwicklung e.V., Goseriede 13a, D-30159 Hannover, Germany, www.his-he.de

Dr. Maren Lübcke is head of the Higher Education Management department of the HIS-Institute of Higher Education Development (HIS-HE) in Hannover. Her consulting and research focus at HIS-HE is the digitization of research and teaching at universities. She has worked on various national and international research projects and is author of various publications in this field.
luebcke@his-he.de

Dr. Mathias Stein is consultant and project manager in the Higher Education Management department of the HIS-Institute of Higher Education Development (HIS-HE) in Hannover. His focus is on digitalization, cybersecurity and processes in universities administration and with respect to the student life cycle.
stein@his-he.de