Jacek Maślankowski, PhD
Faculty of Management
University of Gdansk, Poland
ORCID: 0000-0003-0357-2736
e-mail: jacek.maslankowski@ug.edu.pl,

Dorota Majewicz, PhD
Koszalin University of Technology, Poland
ORCID: 0000-0003-4568-3549
e-mail: dorota.majewicz@tu.koszalin.pl

CYBERSECURITY AND HIGHER EDUCATION INSTITUTIONS. WEBSITE CONTENT-BASED STUDY

Abstract

The contemporary era is characterized by an unprecedented prevalence of cybersecurity concerns. The proliferation of computers, mobile devices, and the Internet has markedly increased the frequency with which the term "cybercrime" appears in media discourse. The repercussions of insufficient cybersecurity awareness can manifest in significant financial losses and reputational damage. Therefore, it is crucial to examine the challenges associated with cybercrime and cybersecurity. This paper aims to investigate how universities communicate cybersecurity issues. To achieve this, a Big Data infrastructure was employed to perform web scraping of cybersecurity-related content disseminated by higher education institutions. The study focuses on the primary challenges universities encounter regarding the protection of data and the enhancement of institutional reputation. Based on the findings, a suggestion for effectively communicating cybersecurity issues within the university context is proposed.

Keywords: cyberattack, cybercrime, cyberthreat, security incident, big data

INTRODUCTION

Research indicates that higher education institutions (HEIs) face substantial cybersecurity challenges and must develop effective communication strategies to enhance awareness among their stakeholders. Potgieter[1] (2019) suggests utilizing social media platforms such as Facebook and YouTube, in addition to institutional websites and emails, as key channels for disseminating cybersecurity awareness to students. To foster a robust cybersecurity culture, HEIs are advised to adopt comprehensive system-wide approaches, including strengthening governance structures, reassessing key performance

[1] P.C. Potgieter, The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. "International Conference on the Internet, Cyber Security and Information Systems", 2019.

indicators, and implementing targeted awareness campaigns[2]. The effective communication of cybersecurity risks is essential, with recommendations emphasizing the importance of adopting trustworthy and user-friendly security practices across diverse contexts[3]. Additionally, institutional factors significantly impact cybersecurity disclosures, as demonstrated by variations between Chinese cross-listed firms and U.S. domestic firms. The Chinese regulatory framework's externalization of cybersecurity results in lower disclosure levels for Chinese firms, whereas the market valuation of such disclosures is sensitive to shifts in institutional perceptions[4].

The following research questions are explored in this paper:

- RQ1: How do higher education institutions address cybersecurity on their official websites?
- RQ2: Do higher education institutions provide students with information regarding potential cybersecurity threats?
- RQ3: Is it feasible to access free cybersecurity courses through higher education institutions to enhance knowledge on cybersecurity issues?

Based on these research questions, the following hypotheses have been formulated:

- H1: The majority of cybersecurity references on higher education institutions' websites pertain primarily to cybersecurity-related academic programs and studies.
- H2: There is minimal or no information available on higher education institutions' websites regarding cybersecurity incidents within the institution.
- H3: It is unlikely that up-to-date information on cybersecurity threats and vulnerabilities can be found on higher education institutions' websites.

This paper is structured into six sections. Following the introduction, the first section provides a literature review. The second section outlines the methodologies employed in conducting a case study. The third section presents the results and discussion and proposes a framework for effective communication of cybersecurity issues by HEIs. The final section concludes with a summary of findings and implications.

[2] E.C. Cheng, T. Wang, Institutional Strategies for Cybersecurity in Higher Education Institutions, “Information”, 2022, Vol. 13, No. 192.
[3] J.R.C. Nurse, Effective Communication of Cyber Security Risks. “7th International Scientific Conference on Security and Protection of Information”, 2013.
[4] T. Barry, J. Jona, N.S. Soderstrom, The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms, “SSRN Electronic Journal”, 2021.

LITERATURE AND LEGAL ACTS REVIEW

There are two different views on the cybersecurity in higher education institutions. One role is to offer courses and educate people on how to be safe in the world dominated by cyberthreats. Second role is to inform students, staff and third parties on the incidents that occurred in the institution.

Concerning the first role of higher education institutions, cybersecurity is an important factor at higher education institutions, both in redesigning the curriculum at Universities due to its high importance in nowadays world[5] but also in areas of risk management[6]. In this sense, IT governance nevertheless it is centralized or not, should incorporate cybersecurity issues[7]. In particular, researchers processing valuable data in their research are vulnerable to cyberattacks[8].

Cybersecurity programs in higher education institutions are gaining increasing importance due to the rising threats and vulnerabilities in this sector. European universities are actively working to integrate security-building competencies into their curricula[9]. Despite broad consensus on critical issues such as mission-critical assets and common vulnerabilities, empirical research on cybersecurity risks within higher education remains limited[10]. In response to the growing demand for qualified cybersecurity professionals, academic institutions are encouraged to prioritize cybersecurity topics within information technology education programs[11]. The "Prepare, Defend, Act" framework has been proposed as a model for structuring cybersecurity emphases in curricula. Higher education institutions face distinct challenges in implementing effective cybersecurity measures due to the complexity and decentralization of their networks, as well as the diverse

[5] G. Towhidi, J. Pridmore, Aligning Cybersecurity in Higher Education with Industry Needs, "Journal of Information Systems Education", 2023, No. 34(1), pp. 70–83.
[6] B. M. Dioubate, W.D. Wan Norhayate, Z.F. Anwar, S. Fauzilah, H.M. Faiz, Lee Ooi Hai, The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions, "Jurnal Pengurusan", 2023, No. 67, pp. 1–12. https://doi.org/10.17576/pengurusan-2023-67-03
[7] C.-W. Liu, P. Huang, H. C. Lucas, Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions, "Journal of Management Information Systems", 2020, No. 37(3), pp. 758–787.
[8] D. Mukherjee, Cybersecurity In The Education Sector: Higher education has long been a target for cyberattacks due to research programs with potentially valuable data, "CIO&Leader", 2022, No. 11(9), pp. 25–26.
[9] N. Dragoni, A. Lluch Lafuente, F. Massacci, A. Schlichtkrull, Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs, "IEEE Security & Privacy", 2021, No. 19, pp. 81-88. DOI:10.1109/MSEC.2020.3037446
[10] J.B. Ulven, G. Wangen, A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 2021, Vol. 13, No. 39. DOI:10.3390/fi13020039
[11] D.C. Rowe, B.M. Lunt, J.J. Ekstrom, The role of cyber-security in information technology education, "Conference on Information Technology Education", 2011, DOI:10.1145/2047594.2047628

nature of their stakeholders[12]. Given that these institutions manage vast amounts of sensitive data and are heavily reliant on technological infrastructure, comprehensive cybersecurity programs and awareness initiatives are crucial to mitigate the risks posed by evolving threats.

According to the data by Statistics Poland, in 2023/2024 academic year there were 9 higher education institutions offering field of study named "Cybersecurity" and in total 21 HEIs offering fields of study related to cybersecurity on Bachelor or Master degree[13].

In relation to the second role of higher education institutions (HEIs), cybersecurity threats present substantial challenges due to the intricate nature of their networks, decentralized operational structures, and the vast repository of sensitive data they manage[14]. Predominant threats include hacking, phishing, ransomware, distributed denial-of-service (DDoS) attacks, and identity theft. The susceptibility of HEIs is exacerbated by human factors, as both staff and students frequently demonstrate insufficient awareness of fundamental cybersecurity protocols[15]. A systematic review has highlighted a paucity of empirical research focused specifically on cybersecurity risks within HEIs; however, there is significant consensus on key vulnerabilities and challenges[16]. To mitigate these risks, it is recommended that HEIs adopt a comprehensive institutional approach, encompassing the enhancement of governance frameworks, reevaluation of cybersecurity key performance indicators (KPIs), clarification of policies, implementation of awareness programs, and the deployment of advanced security mechanisms. Furthermore, HEIs must also anticipate emerging threats, such as AI-driven cyberattacks, and prioritize the security of mobile devices and encryption practices[17].

Regarding the legal acts, higher education institutions in Poland had to implement the legal acts on the cybersecurity. It is based on the Legal Act on National Cybersecurity System in Poland[18]. The cybersecurity incidents first and foremost should be reported within 24 hours by the system provided by the central government which is available on the website[19]. For instance, in

[12] A.H. Ridha, M.A. AlDhamen, Cyber Security Awareness for Education Institutions, "International Journal of Advanced Research in Computer and Communication Engineering", 2023, Vol. 12, Issue 2, DOI:10.17148/ijarcce.2023.12201

[13] https://stat.gov.pl/obszary-tematyczne/edukacja/edukacja/szkolnictwo-wyzsze-w-roku-akademickim-20232024,8,10.html, as of 27.09.2024

[14] A.H. Ridha, M.A. AlDhamen, Cyber Security Awareness for Education Institutions, "International Journal of Advanced Research in Computer and Communication Engineering", 2023, Vol. 12, Issue 2, DOI:10.17148/ijarcce.2023.12201

[15] O. Trofymenko, N. Loginova, M. Serhii, Y. Dubovoil, Cyberthreats In Higher Education, *"Cybersecurity: Education, Science, Technique"*, 2022, No. 16, pp. 76-84.

[16] J.B. Ulven, G. Wangen, A Systematic Review of Cybersecurity Risks in Higher Education, "Future Internet", 2021, Vol. 13, No. 39, DOI:10.3390/fi13020039

[17] E.C. Cheng, T. Wang, Institutional Strategies for Cybersecurity in Higher Education Institutions, "Information", 2022, Vol. 13, No. 192.

[18] ACT of 5 July 2018 on the National Cybersecurity System, Dz.U. z 2024 r. poz. 1077, 1222.

[19] https://www.gov.pl/web/baza-wiedzy/zglaszanie-incydentow, as of 27.09.2024

Lodz Film School in Poland according to its internal regulation “University employees are required to report incidents they notice and to record all details related to the incident “[20].

METHODS

The data collection method employed in this study was web scraping. The technology used was Python language with NoSQL database to store websites for data processing and analysis. It is a typical Big Data related infrastructure used for web content analysis.

Initially, a sampling frame was constructed based on the Register of Higher Education and Science System Institutions, as provided by the Ministry of Higher Education and Science in Poland. Institutional data was current as of September 2024, and the web scraping process was conducted during the same period. Further details regarding the sampling frame are provided in Table 1.

Table 1. Sample frame in the survey

Specification	Number
Total number of institutions	823
of which public and private higher education institutions	517
of which able to scrape	460
of which scraped	408

Source: own study.

Table 1 provides an overview of the institutions included in the study. Out of a total of 823 higher education and science institutions, of which scientific institutions, church-affiliated institutions, and other entities not classified as public or private higher education institutions were excluded. As a result, 517 were classified as either public or private higher education institutions. From these, web scraping was conducted on 460 institutions, of which 52 units did not respond to robot requests. The table highlights the subset of institutions that were eligible for and included in the web scraping process.

Prior to scraping, the robots.txt file of each website was checked to verify whether scraping was permitted by the site owner. The scraping process focused on identifying the terms "cyberbezpieczeństwo" (in the Polish version of the website) or "cybersecurity" (in the English version). To improve the

[20] https://bip.filmschool.lodz.pl/userfiles2/Zarz%C4%85dzenie%20nr%2048_2021%20Za%C5%82%C4%85cznik%20nr%201.pdf, as of 27.09.2024

accuracy of keyword detection, lemmatization and stemming techniques were applied.

Data was scraped up to the second level of each website, meaning that all links from the homepage were included, as well as the content of subpages linked directly from the main page. Content not accessible from the homepage was excluded from the analysis. Data was analysed in two versions – raw data and processed, i.e. rendered to the web browser capabilities.

RESULTS AND DISCUSSION

The analysis was to find and interpret the information on cybersecurity in Polish and English language in webpages on the first and second level depth. Our analysis shows that most of the Higher Education Institution do not refer to cybersecurity at the most visited parts of webpages. The results are shown in Table 2.

Table 2. Reference to cybersecurity on HEI webpages

Specification	Number
Number of scraped institutions	408
Information on page or subpage on cybersecurity	47

Source: own study.

Table 2 presents the results of the web scraping process. Out of 408 institutions where data was successfully scraped, 47 institutions featured information related to cybersecurity either on their homepage or subpages. This highlights the relatively small proportion of institutions that provide cybersecurity-related content on their websites.

The majority of references in the dataset pertain to academic programs offered by higher education institutions (HEIs), indicating the relevance of cybersecurity as a topic of study. The data reveals that many HEIs are offering courses that address various aspects of cybersecurity. Among the most commonly referenced programs is Cybersecurity Management, with some institutions also providing advanced-level courses, such as MBA programs focused on cybersecurity. Additionally, certain HEIs offer cybersecurity courses specifically tailored to fields like public administration and national security.

Only a select number of institutions (nine, as identified in the survey) address practical cybersecurity issues beyond academic offerings. These include video tutorials on maintaining cybersecurity in everyday contexts. A few institutions also highlighted their specialized cybersecurity centers, such as those focused on maritime cybersecurity, aligning with their institutional specializations.

Some HEIs actively promote cybersecurity awareness through events such as expert-led lectures and hackathons, which serve as effective tools for raising awareness and emphasizing the importance of cybersecurity.

Despite these efforts, the survey results indicate that few institutions report cybersecurity incidents on their websites. This may be due to concerns that such disclosures could negatively impact the institution's reputation. Conversely, institutions that publish cybersecurity incidents may enhance their credibility by demonstrating transparency. However, based on the available data from institutional websites, it is difficult to accurately estimate the actual number of cybersecurity incidents, as many may go unreported.

In conclusion, the research questions posed in this study can be addressed in alignment with the findings from the dataset and the observed practices of HEIs regarding cybersecurity.

RQ1: How do higher education institutions address cybersecurity on their official websites?

As previously noted, the majority of the data pertains to cybersecurity courses offered by higher education institutions. A limited number of institutions report cybersecurity incidents, based on the information available on their websites as of September 2024.

RQ2: Do higher education institutions provide students with information regarding potential cybersecurity threats?

In total, nine institutions were found to have organized events or provided instructional content on their homepages or associated subpages (with links examined up to the second level of depth) related to enhancing cybersecurity awareness. These resources included guidance on how to improve personal cybersecurity practices and respond effectively to various cybersecurity incidents.

RQ3: Is it feasible to access free cybersecurity courses through higher education institutions to enhance knowledge on cybersecurity issues?

While additional information may be available, not all institutions reported cybersecurity-related events or incidents on their websites. It is likely that more cybersecurity activities or updates occur throughout the academic year; however, at the time of this study, it was not possible to gather comprehensive data on specific incidents.

In accordance with Hypothesis H1, formulated in this paper, the findings confirm that the majority of cybersecurity references on higher education institution (HEI) websites primarily focus on academic programs and courses related to cybersecurity. Hypothesis H2 is also supported, indicating that minimal or no information is available regarding cybersecurity incidents within HEIs. Regarding Hypothesis H3, it appears unlikely that up-to-date information on cybersecurity threats and vulnerabilities is available on HEI websites, including on the main website and in the Public Information Bulletin (Biuletyn Informacji Publicznej, BIP).

Based on the results of the survey and supporting literature, we propose improvements in the communication of cybersecurity issues at higher education institutions. Specifically, it would be beneficial to have a dedicated

section on the main page of HEI websites addressing cybersecurity matters. It is essential that students are informed about potential cybersecurity risks, especially as many use shared computers in computer labs. Our observations over recent years have revealed recurring issues, such as students neglecting to log out from university services (e.g., educational portals), allowing subsequent users access to their profiles. Similarly, students frequently forget USB drives in shared computers, which poses additional security risks. Another notable issue involves difficulties logging out of Microsoft shared services in standalone MS Office applications, where the login process is integrated into the Windows operating system.

These observations highlight the need for HEIs to raise cybersecurity awareness among students, with a focus on institution-specific resources. In this regard, cybersecurity education cannot be generalized as standard coursework; rather, it should be tailored to the infrastructure of each university. We recommend mandatory cybersecurity courses specifically designed for students that address the university's unique resources and risks.

While faculty and staff typically undergo mandatory training on data protection and, to some extent, cybersecurity, our recommendations are largely focused on students. One of the most effective methods for communicating cybersecurity issues is through regular updates via social media and institutional websites. However, to ensure communication is effective, we advocate for regular, short courses that address security issues specific to the HEI, including recent security incidents. A single course at the beginning of the academic year is insufficient, as students may not retain all details. Regular reporting on cybersecurity issues should be a routine practice for HEIs, not perceived as a threat to their reputation, but rather as a means to build trust with the student body and staff.

CONCLUSIONS

The Big Data survey conducted in this study successfully addresses all three research questions and validates the corresponding hypotheses. The findings reveal that higher education institutions (HEIs) require improvements in their communication of cybersecurity practices to students and staff engaged with institutional resources. The primary objective of the paper—assessing the communication methods related to cybersecurity on HEI websites—has been achieved, and we were able to comprehensively catalog these methods.

The results indicate that most cybersecurity-related content on HEI websites is focused on the academic programs in cybersecurity offered by the institution. Some HEIs feature dedicated laboratories or centers for cybersecurity research, while only a limited number provide free videos or instructions on cybersecurity issues through their websites. Although the communication of cybersecurity information via institutional websites is generally efficient, it is acknowledged that not all details regarding cybersecurity incidents are disseminated through official communication

channels. This study proposes enhancing the overall communication of cybersecurity issues through HEI websites.

Based on the findings, we recommend the development of a comprehensive framework for HEIs to systematically report cybersecurity issues on their websites and, where applicable, on social media platforms. The proposed framework should also incorporate regular short courses or instructional materials that address institution-specific cybersecurity threats. For example, if an HEI utilizes cloud computing services, it should provide continuous updates and guidance on cyber threats related to that technology. Publishing such information regularly would naturally enhance cybersecurity awareness among students.

References

Barry T., Jona J., Soderstrom N.S., The Impact of Country Institutional Factors on Firm Disclosure: Cybersecurity Disclosures in Chinese Cross-Listed Firms, "SSRN Electronic Journal", 2021.

Cheng E.C., Wang T., Institutional Strategies for Cybersecurity in Higher Education Institutions, "Information", 2022, Vol. 13, No. 192.

Dioubate B. M., Wan W.D. Norhayate, Anwar Z.F., Fauzilah S., Faiz H.M., Lee Ooi Hai, The Role of Cybersecurity on the Performance of Malaysian Higher Education Institutions, "Jurnal Pengurusan", 2023, No. 67, pp. 1–12. https://doi.org/10.17576/pengurusan-2023-67-03

Dragoni N., Lluch Lafuente A., Massacci F., Schlichtkrull A., Are We Preparing Students to Build Security In? A Survey of European Cybersecurity in Higher Education Programs, "IEEE Security & Privacy", 2021, No. 19, pp. 81-88. DOI:10.1109/MSEC.2020.3037446

Liu C.-W., Huang P., Lucas H. C., Centralized IT Decision Making and Cybersecurity Breaches: Evidence from U.S. Higher Education Institutions, "Journal of Management Information Systems", 2020, No. 37(3), pp. 758–787.

Mukherjee D., Cybersecurity In The Education Sector: Higher education has long been a target for cyberattacks due to research programs with potentially valuable data, "CIO&Leader", 2022, No. 11(9), pp. 25–26.

Nurse J.R.C., Effective Communication of Cyber Security Risks. "7th International Scientific Conference on Security and Protection of Information", 2013.

Potgieter P.C., The Awareness Behaviour of Students on Cyber Security Awareness by Using Social Media Platforms: A Case Study at Central University of Technology. "International Conference on the Internet, Cyber Security and Information Systems", 2019.

Ridha A.H., AlDhamen M.A., Cyber Security Awareness for Education Institutions, “International Journal of Advanced Research in Computer and Communication Engineering”, 2023, Vol. 12, Issue 2, DOI:10.17148/ijarcce.2023.12201

Rowe D.C., Lunt B.M., Ekstrom J.J., The role of cyber-security in information technology education, “Conference on Information Technology Education”, 2011, DOI:10.1145/2047594.2047628

Towhidi G., Pridmore J., Aligning Cybersecurity in Higher Education with Industry Needs, “Journal of Information Systems Education”, 2023, No. 34(1), pp. 70–83.

Trofymenko O., Loginova N., Serhii M., Dubovoil Y., Cyberthreats In Higher Education, “Cybersecurity: Education, Science, Technique”, 2022, No. 16, pp. 76-84.

Ulven J.B., Wangen G., A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet, 2021, Vol. 13, No. 39. DOI:10.3390/fi13020039

ACT of 5 July 2018 on the National Cybersecurity System, Dz.U. z 2024 r. poz. 1077, 1222.

https://www.gov.pl/web/baza-wiedzy/zglaszanie-incydentow, as of 27.09.2024
https://bip.filmschool.lodz.pl/userfiles2/Zarz%C4%85dzenie%20nr%2048_2021%20Za%C5%82%C4%85cznik%20nr%201.pdf, as of 27.09.2024

https://stat.gov.pl/obszary-tematyczne/edukacja/edukacja/szkolnictwo-wyzsze-w-roku-akademickim-20232024,8,10.html, as of 27.09.2024

CYBERBEZPIECZEŃSTWO A INSTYTUCJE SZKOLNICTWA WYŻSZEGO. BADANIE TREŚCI STRON INTERNETOWYCH SZKÓŁ WYŻSZYCH

Streszczenie

Współczesność charakteryzuje się niespotykanym dotąd rozpowszechnieniem obaw o cyberbezpieczeństwo. Rozprzestrzenianie się komputerów, urządzeń mobilnych i Internetu znacznie zwiększyło częstotliwość, z jaką termin „cyberprzestępczość” pojawia się w dyskursie medialnym. Skutki niewystarczającej świadomości cyberbezpieczeństwa mogą objawiać się znacznymi stratami finansowymi i szkodami dla reputacji. Dlatego też kluczowe jest zbadanie wyzwań związanych z cyberprzestępczością i cyberbezpieczeństwem. Niniejszy artykuł ma na celu zbadanie, w jaki sposób uniwersytety komunikują kwestie cyberbezpieczeństwa. Aby to osiągnąć,

wykorzystano infrastrukturę Big Data do wykonania web scrapingu treści związanych z cyberbezpieczeństwem rozpowszechnianych przez instytucje szkolnictwa wyższego. Badanie koncentruje się na głównych wyzwaniach, z jakimi borykają się uniwersytety w zakresie ochrony danych studentów i poprawy reputacji instytucji. Na podstawie ustaleń zasugerowano metody skutecznej komunikacji kwestii cyberbezpieczeństwa w szkołach wyższych.

Słowa kluczowe: cyberatak, cyberprzestępstwo, cyberzagrożenie, incydent bezpieczeństwa, big data.