REGIONAL
CYBER LABS

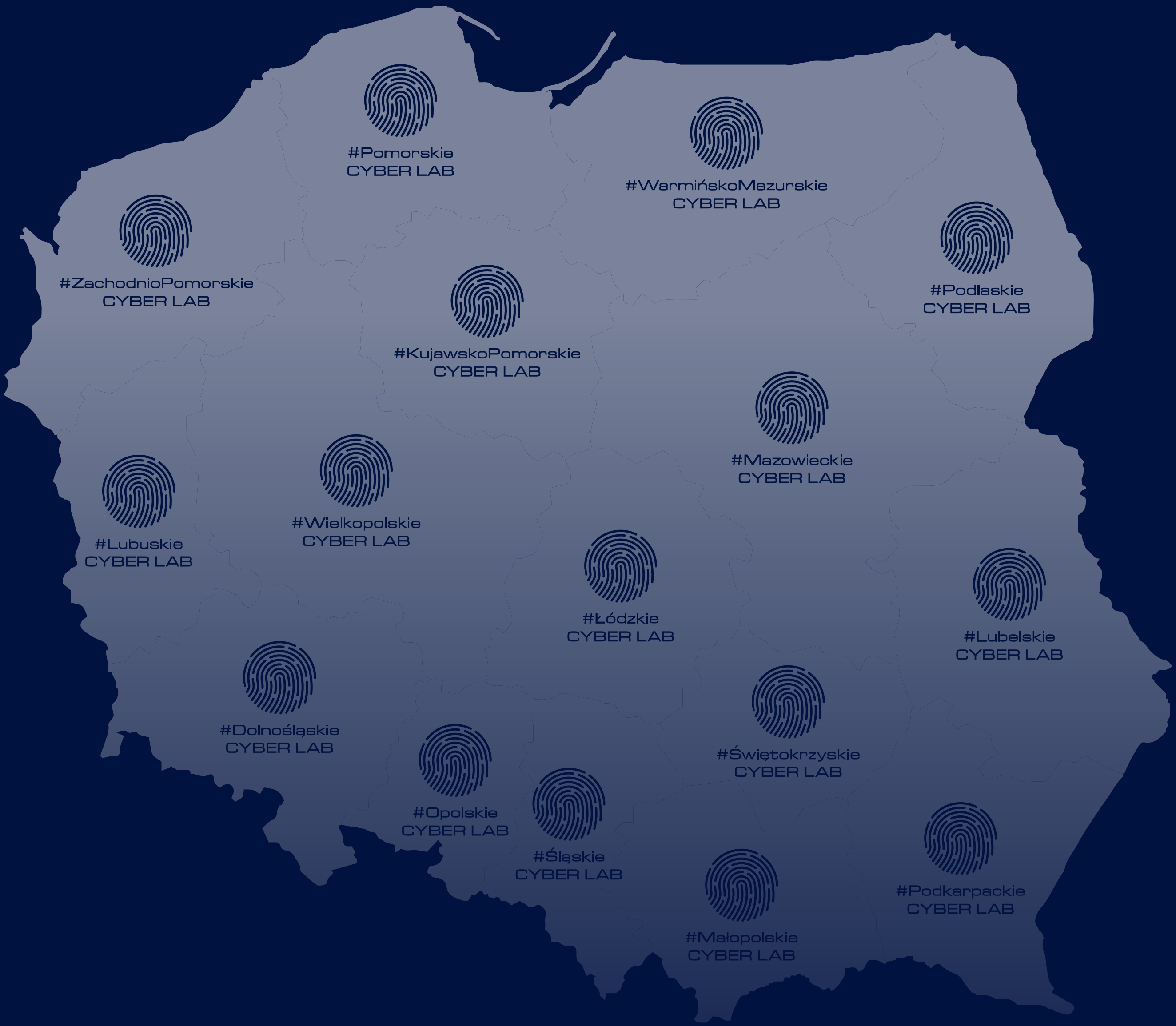
REPORT
A NEW ROADMAP FOR CYBERSECURITY EDUCATION
2020-2021

The Bridge Foundation

CYBER SECURITY
CHALLENGE
PL/2020

A NEW ROADMAP FOR CYBERSECURITY EDUCATION

REGIONAL CYBER LABS



Nationwide student assessment report promoting an interdisciplinary approach to cybersecurity education in Polish universities as a key component in the national security ecosystem. This project was carried out as a part of the Regional Cyber Labs initiative, an innovative platform for cybersecurity education. Participating students represent the following university domains: IT/engineering, law, business, medical and military studies.

PREFACE

The dynamic development of advanced technologies and accelerating digitalization impact all aspects of our lives, including the field of education. The effect of these changes depends on how we manage the digital transformation, a process where higher learning plays an essential role.

The implementation of content, in the university curricula, that gives students the knowledge and competencies expected by various stakeholders presents a formidable challenge.

This report is an invitation for academic and student circles, public institutions and the private sector to reflect and exchange on this vital topic. The student recommendations can positively influence the ability of academic institutions to respond effectively to the needs of the market. This can be achieved by implementing educational measures that support the digital transformation.

The study domains represented in the report (IT/Engineering, law, business, medicine, and military) are fundamental to the process of digital transformation for the coming decade. The review across these fields, based on the link between technological progress and cybersecurity, creates an opportunity for boosting and better employing the intellectual capital of students. A key aspect in this process is to promote a mutually enriching student – teacher relationship.

The experience gained and the potential created during the Cybersecurity Challenge PL 2020, organized under the patronage of the Ministry of Digital Affairs, Government Center for Security, and ISSA Poland laid the foundations for this document. The project saw students from five domains joining forces: IT/Engineering, law, business, medicine, and military. Sixteen interdisciplinary teams, each representing their voivodeship, played the role of "tiger groups" - government advisors - during a cyber crisis impacting the nation and its critical infrastructure.

Students from 65 universities participated in this innovative competition where they addressed the strategic, technological, regulatory and communication aspects of a massive cyber-attack. The challenge opened the door for new initiatives including the creation of Regional Cyber Labs - an agora for young leaders interested in developing an expertise in cybersecurity.

Their collaborative effort to prepare this report represents their first project. The authors include challenge participants and members of student research circles.

I thank all those who joined forces in the preparation of this document. Experts, institutions, ambassadors and especially the students for their dedication and professionalism. Through this project they serve the greater common good. Having taken their own generation into account, they also considered the wider social spectrum which is perfectly depicted in the statement that cybersecurity concerns us all - from junior to senior.

I therefore invite you to read these pages and join this discussion while keeping in mind the following metaphor: cybersecurity education is like a marathon, not a sprint. It calls for a sustained effort, crosscutting approach and questions that lead to novel thinking and action.

Margo Koniuszewski
President of The Bridge Foundation

LOCAL AND INTERNATIONAL REACH

REGIONAL CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland

The report is part of a larger discourse on shaping cybersecurity education in a local, regional and international context.

Nationwide, it supports the objectives of the Cybersecurity Strategy of the Republic of Poland for 2019/24 and the National Security Strategy (in the field of cybersecurity). It raises social awareness and builds critical competencies in cybersecurity and strengthens the national security ecosystem by promoting best practices.

Through its international dimension, it influences the shaping of policies conducive to a safe and orderly global digital transformation. It pursues the objectives resulting from Poland's membership in international organizations including the EU, UN, OECD and NATO, in the field of education: building interdisciplinary competencies and knowledge/experience sharing with a wide range of stakeholders from academia, business, public institutions, to NGOs and international organizations.

METHODOLOGY

REGIONAL CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland

Student recommendations put forward the interdisciplinary nature of the cybersecurity ecosystem. They follow a review of the university curricula and survey of their peers currently enrolled in IT, law, business, medicine and military studies at universities across Poland. The report also contains comments from the academic community and experts in the relevant fields.

In each domain, students prepared their own analysis of existing cybersecurity content that was further investigated and enriched through student consultations. The report is therefore the fruit of a wide-reaching collective effort.

It must be emphasized that the assessment and recommendations were developed by students independently - without any faculty involvement. The professors engaged in the project had a supportive role and did not influence the report content.

For each domain, two student-coordinators acted as group leaders to manage the review, recommendations and report preparation process.

DOMAIN COORDINATORS

Cybersecurity is key to overall security in the 21st century.

AGATA ZALEWSKA, Ambassador #WarmińskoMazurskieCyberLab

Student University of Warmia and Mazury in Olsztyn, Faculty of Law and Administration

In the digital era we need an interdisciplinary approach to cybersecurity education.

ANDRZEJ PORĘBSKI, Ambassador #MałopolskieCyberLab

Student Jagiellonian University in Cracow, Faculty of Law and Administration
and AGH University of Science and Technology, Faculty of Management

The digital transformation comes with opportunities and challenges. Good navigation is essential to harness its possibilities.

NATALIA BRONDER, Ambassador #OpolskieCyberLab

Student Opole University of Technology, Faculty of Electrical Engineering Automatic Control and Informatics

The project is nationwide in scope and resonates internationally.

MATEUSZ JACHNIAK, Ambassador #DolnośląskieCyberLab

Student Wrocław University of Science and Technology, Faculty of Fundamental Problems of Technology

We share the experience gained during Cybersecurity Challenge PL2020.

MARTA LEWANDOWSKA, Ambassador #WielkopolskieCyberLab

Student Poznań University of Technology, Faculty of Engineering Management

We go beyond the traditional patterns of thinking and acting.

KAMIL CHMURA, Ambassador #LubelskieCyberLab

Student Maria Curie-Skłodowska University in Lublin, Faculty of Economics

Synergy from the project represents a tangible, innovative asset.

JULIA MAKUCH, Ambassador #DolnośląskieCyberLab

Student Wrocław Medical University, Faculty of Medicine

This report opens a new world of possibilities in cybersecurity education.

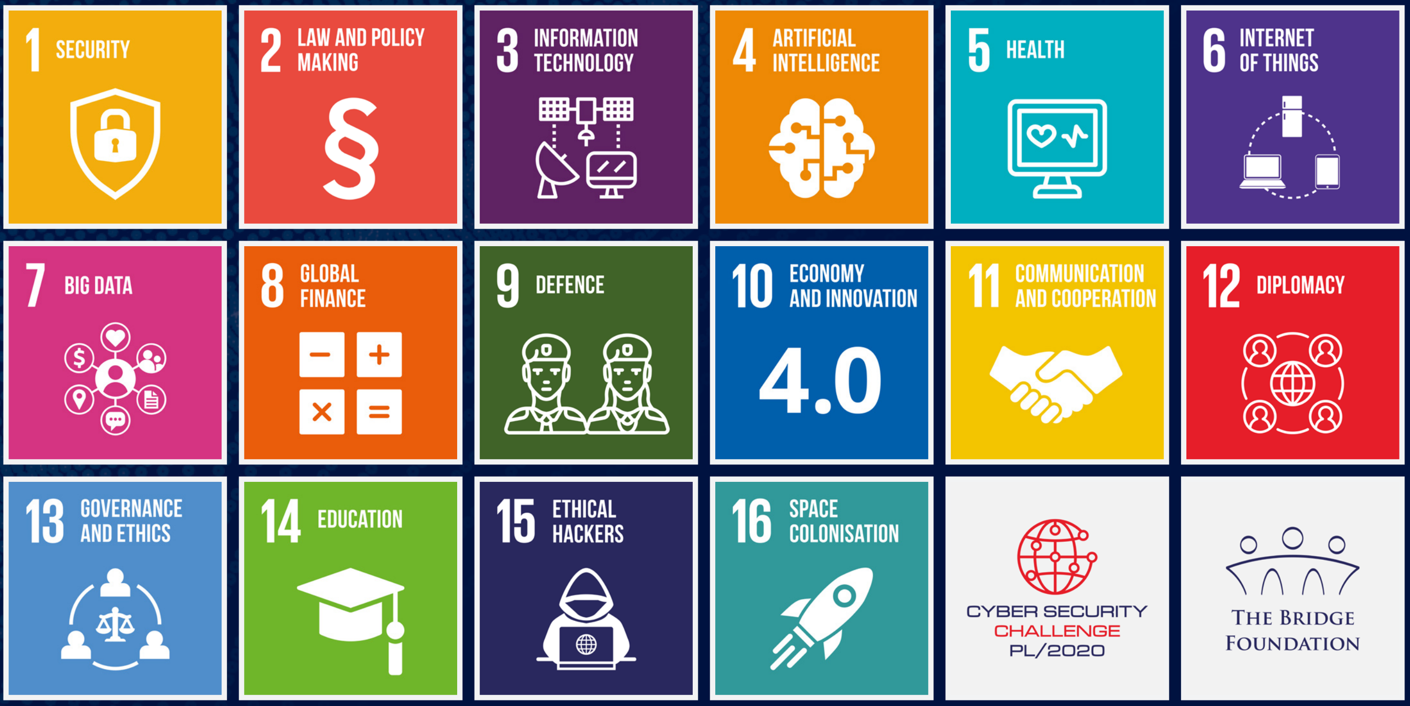
MATEUSZ GUZIAK, Ambassador #PomorskieCyberLab

Student Medical University of Gdańsk, Faculty of Medicine

STUDENT RECOMMENDATIONS

132 students representing 35 universities actively engaged in preparing this report and its recommendations. Comments from academia and experts complement the conclusions for each of the represented domains: Information Technology, Business, Medicine, Law and the Military.

#CyberSecurityEcosystem


1 SECURITY

2 LAW AND POLICY MAKING

3 INFORMATION TECHNOLOGY

4 ARTIFICIAL INTELLIGENCE

5 HEALTH

6 INTERNET OF THINGS

7 BIG DATA

8 GLOBAL FINANCE

9 DEFENCE

10 ECONOMY AND INNOVATION 4.0

11 COMMUNICATION AND COOPERATION

12 DIPLOMACY

13 GOVERNANCE AND ETHICS

14 EDUCATION

15 ETHICAL HACKERS

16 SPACE COLONISATION

CYBER SECURITY CHALLENGE PL/2020

THE BRIDGE FOUNDATION

INFORMATION TECHNOLOGIES

REGIONAL CYBER LABS

Mateusz Rędzia

Wrocław University of Science and Technology
Faculty of Electronics

RECOMMENDATIONS
INFORMATION TECHNOLOGIES DOMAIN

Source materials were collected as part of the curriculum analysis carried out by students of ten Polish universities with a technological profile: Cracow University of Technology, Lublin University of Technology, Łódź University of Technology, Opole University of Technolog, Poznań University of Technology, Silesian University of Technology, Nicolaus Copernicus University in Toruń, University of Warmia and Mazury in Olsztyn, Wrocław University of Science and Technology, University of Zielona Góra.

Engineering School Domain Executive Summary
(pages 8 to 16 in Polish version of the report)

With the rapid development of the digital economy and society, one could expect for cybersecurity to feature prominently in any technological innovation. Yet, as programmers, digital innovators and entrepreneurs are hard pressed to innovate ahead of competitors - and as cheaply as possible - security often takes a backseat, opening the door to attacks and breaches.

As we could expect, the recent shift to online activities coincided with an unprecedented growth in cybercrime – as reported by the FBI, confirming the prophetic words of IBM Chairman, Ginni Rometty that "Cybercrime is the greatest threat to every company in the world." With the cost of cybercrime expected to reach $6 trillion by 2021, more attention should be given to cybersecurity across all sectors of the economy and it should feature prominently in digital innovation.

The observations of technical university students are consistent with this analysis. They take good note of the priority given to innovation over security in the material covered and the way it is conveyed in their faculties. One of their key recommendations is for security to feature prominently as a crosscutting element throughout technical studies – not only in cybersecurity courses and materials. For them, data breaches at various universities are a symptom that cybersecurity and data privacy considerations are not taken as seriously as they should by universities. They recommend the following priority areas for enhancing the cybersecurity content in the university curricula:

1 — The "cyber-criminal" mind

Students need a better understanding of cyberattacks and the importance of cybersecurity. Simulations and exercises of realistic and multifaceted cyberattacks are a preferred format to illustrate cyberthreats, the importance of interdisciplinary cooperation, and need for prevention. The ability to think 'like a cybercriminal' will help IT professionals prioritize safety, security and prevention in IT innovation and design.

2 — Cybersecurity as a crosscutting feature in technical studies

In addition to dedicated courses on cybersecurity, its importance warrants inclusion across all technical study fields and courses.

3 — Ongoing syllabus review and academic staff qualifications

Given the accelerating pace of change in IT, program content and staff qualifications must be constantly reviewed and updated. The pressures of innovation call for being at the cutting-edge. Self-education and a mutually reinforcing student-lecturer relationship must be encouraged.

RECOMMENDATIONS
INFORMATION TECHNOLOGIES DOMAIN

4 — Operational Compliance and Security

Courses focused on achieving confidentiality, integrity and availability (CIA triad) are essential to raise student awareness about security gaps in systems (database architecture, etc), including unauthorised access (see access rights), importance of testing / security checks, contingency plans and recovery for organisational resilience to become the norm.

5 — User Access Rights

Greater attention must be given to proper user permissions (applications/systems/design), the abuse of Admin accounts, lack of segregation of incompatible duties and excessive privileges (admin/users). Students must understand the least privilege policy as fundamental. Teaching based on concrete examples, case studies and simulations is best to develop good habits.

6 — Cyber-Hygiene

Relevant to all users and particularly IT professionals and software developers. From password managers, two-factor authentication, using software from reliable sources, timely updates and backups, these represent essential knowledge to operate in the digital world.

7 — Awareness training and secure software systems

Insufficient emphasis on safety and security in software development opening the door to abuse, misuse and attacks, including phishing. Students should be exposed to relevant legislations (GDPR, etc.), the importance and ways of securing data (database architecture, etc.) and embedding security and safety from the onset as a standard, not an added element in late stages of development.

RECOMMENDATIONS
INFORMATION TECHNOLOGIES DOMAIN

REPORT CO-AUTHORS INFORMATION TECHNOLOGIES

Natalia Bronder — Faculty of Electrical Engineering Automatic Control and Informatics,
Opole University of Technology
Irmina Chmielowska — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology
Paweł Cyprys — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology
Jakub Czyszczonik — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology
Bartosz Drzazga — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology
Piotr Dudek — Faculty of Electrical and Computer Engineering,
Cracow University of Technology
Mateusz Gąsior — Faculty of Computer, Electrical and Control Engineering,
University of Zielona Góra
Mariusz Górny — Faculty of Electrical and Computer Engineering,
Cracow University of Technology
Mateusz Jachniak — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology
Michał Kobielski — Faculty of Mechanical Engineering, Silesian University of Technology
Kilian Kozioł — Faculty of Mathematics and Computer Science,
University of Warmia and Mazury in Olsztyn
Emanuel Krzysztoń — College III, Kazimierz Wielki University, Bydgoszcz
Piotr Ładoński — Faculty of Electrical, Electronic, Computer and Control Engineering,
Łódź University of Technology
Grzegorz Maksim — Faculty of Electrical Engineering and Computer Science,
Lublin University of Technology
Jan Ziemniewicz — Faculty of Computing and Telecommunications,
Poznań University of Technology
Rafał Sawicki — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology
Gabriel Tański — Faculty of Fundamental Problems of Technology,
Wrocław University of Science and Technology

EXPERT OPINION

Wojciech Wodo, PhD, Eng

Congratulations to all the students for conducting such a thorough analysis. Its results and recommendations are consistent with the views of cybersecurity experts on the subject (vide quoted reports), and the presented suggestions to improve cybersecurity education are supported by concrete solutions and examples.

The dynamics of technological development means knowledge and solutions quickly become outdated. Nowadays, one of the biggest threats is being oblivious to this fact. A remedy for such mindset is continuous education that raises awareness about cybersecurity (awareness training).

In the past, hardly anyone could use a computer. Today, basic digital skills are essential. This is why we should define a new set of skills for tomorrow, or perhaps even for today (those who exist and operate in two worlds: the real and the digital). These include navigating in the digital world and using its services consciously and safely. Nowadays, nobody is surprised by smartphone and smartwatch cashless payments, filing a tax return online, or submitting an application with an electronic signature such as the Trusted Profile on the ePUAP platform. But do we fully understand the risks connected with using these services and how to stay safe?

Students identified phishing as one of the fundamental cyber-attacks of the modern world. It is an automated, mass-scale activity, but it is also only the tip of the iceberg. Hence, it is necessary to define new abilities and skills, which every user of the internet and other digital services must possess. Moreover, it is also crucial that a new teaching program, including the above mentioned topics, is introduced in the earliest stages of education (elementary school).

The authors addressed the lack of cybersecurity education in the courses offered as a part of ICT studies. As an academic teacher I agree with their assessment, however, we also need to consider the bigger picture. If we include certain topics in the curriculum, we would have to remove others given the limited number of hours available. Another question is if we should expand the number of elements in the courses we teach, but present them in less detail (T-shape approach), or introduce fewer topics in more detail (I-shape approach). Unfortunately, these two approaches exclude each other. Another issue is the level of knowledge and awareness students have when they arrive at university. If they do not possess the necessary basics there is no foundation for further learning.

I fully second student recommendations regarding minimizing user permissions, implementing the least privilege policy, and adapting the opt-in approach, instead of the opt-out. As a general rule, we should limit user permissions to the necessary minimum. If a need for expanding them arises, an authorized administrator must take this responsibility.

From the onset, security should be included in designing and creating information systems. The security, safety, and privacy by design approach will assure that safety features are not added in a hurry to an already designed solution but constitute an integral and well-thought-through component. If we do not teach this approach to our IT, Electronics and Telecommunications graduates (and related fields), we will face a ticking time bomb of our own design.

Wojciech Wodo

Assistant in the Department of Fundamentals of Computer Science at the Wrocław University of Technology, TOP 500 Innovator, University of California, Berkeley.

BUSINESS

Milena Bobińska

Military University of Technology
Faculty of Security Logistics and Management

RECOMMENDATIONS BUSINESS DOMAIN

Source materials were collected as part of a curriculum review carried out in cooperation with students from the following eleven Polish business and economic universities: University of Białystok, University of Gdańsk, Kardynał Stefan Wyszyński University in Warsaw, University of Łódź, Maria Curie-Skłodowska University in Lublin, Nicolaus Copernicus University in Toruń, University of Rzeszów, University of Warsaw, University of Warmia and Mazury, University of Wrocław.

Business School Domain Executive Summary

(pages 19 to 27 in Polish version of the report)

With two years of digital transformation taking place in a few months, the ongoing crisis is propelling the digital economy forward. E-commerce, e-business and e-health are here. Omnipresent and lightning speed 5G connectivity is the next promise that will make the Internet of Things (IoT), driverless cars and the 4.0 economy a reality. Throughout, business is at the forefront of these transformations and business students know that digital literacy and cybersecurity are crucial for their personal and professional future. They call for business schools to equip them with relevant and up-to-date knowledge and skills to thrive in the digital economy.

Hence, business school students reviewed their university curricula and questioned their peers on the presence and depth of cybersecurity education in their faculties. They observe insufficient digital economy content despite its growing importance for all sectors. Today already, Economy 4.0 represents 15% of global GDP and is expected to reach 26% by 2040. This massive shift is reshaping the economic landscape and will be critical for the competitiveness of businesses and nations going forward. With data and knowledge as the currency of the digital age, education will play a pivotal role in determining the future competitiveness and prosperity of nations.

For business students, current education in business schools can be enhanced by putting more emphasis on the shift to the digital economy and by underscoring the knowledge and skills needed to thrive in the digital age – including cybersecurity as a key component in corporate governance. They propose to incorporate cybersecurity in the university curricula with pioneering educational initiatives that will promote the topic with the student community and with faculty staff:

1 — Cyber-hygiene

Students and faculty staff should attend mandatory training covering online threats, attack types, and measures to secure their accounts, manage their passwords, VPN solutions, etc. Guidance and content for self-learning from trusted sources should be made available by the university.

2 — Audits and cyber-governance

Raising awareness on the role and importance of audits, cyber-governance, pen testing and how to conduct (cybersecurity) cost-benefit analysis as part of risk management, including considerations of cyber-insurance, should be covered in business schools. Students should learn to evaluate the financial, regulatory and reputational impact of incidents and breaches.

RECOMMENDATIONS BUSINESS DOMAIN

3 — Regulatory Framework

Students must be familiar with key legislation and its business implications (NIS, RODO, National CyberSecurity Act) including the cybersecurity ecosystem structure (CSIRTs, CERT, critical infrastructure operators, key service providers).

4 — Data Security

Data being the currency of the digital age, students must understand data security and privacy concepts, rules, regulations and measures to protect data.

5 — Business Simulations

The format of realistic case studies with examples of attacks and incidents covering response, reporting and prevention is a preferred format for learning. This should include the human element (psychology of cyber-incidents) and best practices before, during and after incidents.

6 — Business Thesis on Cybersecurity

Given the multiplication and potentially catastrophic impact of cyberthreats for enterprise, many students would like to focus their thesis on topics related to the digital transformation and cybersecurity.

REPORT CO-AUTHORS BUSSINES DOMAIN

Kamil Chmura — Maria Curie-Skłodowska University in Lublin, Faculty of Economics
Marcin Guzdek — Wrocław University of Economics and Business, Faculty of Economics and Finance
Kamila Kiełczewska — University of Warmia and Mazury in Olsztyn, Faculty of Economics
Jadwiga Korszniak — University of Technology, Rzeszów Faculty of Management
Marta Lewandowska — Poznań University of Technology, Faculty of Engineering Management
Paweł Lewandowski — Wrocław University of Economics and Business, Faculty of Management
Arek Wawrzyniak — University of Gdańsk, Faculty of Management
Wojciech Zajączkowski — Wrocław University of Economics and Business,
Faculty of Economics and Finance

EXPERT OPINION

Adam Koniuszewski, FCPA, FCA, CFA

I commend the Polish business students for their engagement in this project. It is the first time I encounter such an initiative for which they will be recognized as innovative trendsetters. Their contribution has the potential to become the benchmark for cybersecurity education in business schools of the region and beyond. Their assessment and wide spectrum of practical recommendations from cyber-audits to cyber-insurance illustrates a solid understanding of the functioning of the digital economy where a robust cybersecurity ecosystem is vital and better awareness urgently needed.

Recent months exposed the divide between a struggling industrial economy and a prospering economy 4.0 with its thriving e-commerce / banking / health platforms, cloud services and online-conferencing. And yet, the truly ground-breaking leap forward is still to come.

The 5G and eventually 6G revolutions in network capability will radically increase speed and reduce latency. 5G will be the backbone that will make smart cities, driverless cars, and intelligent and automated factories possible. Zero time-lag will take virtual reality beyond the world gaming and into the mainstream so that a surgeon in Boston can operate a patient in Tokyo through wireless robotics. This will be the golden age of the IoT where applications barely imaginable today will be an essential part of our daily lives tomorrow. This will take us into a new era of technological innovation and wealth creation.

Alongside these formidable advances we must tackle the ever-growing dark specter of cyberthreats to which no country, corporation or organization is immune. Financial institutions, multinationals, governments and even the United Nations are being been hit. And while cyber-challenges are increasingly found on board agendas, organizations struggle to protect themselves and their customers against cyber-threats. These are gaps that auditors, consultants and the insurance industry are racing to fill. This is a new environment where executives don't always understand what they are up against and where seemingly innocent actions can have unexpected and devastating consequences.

For the Fourth Industrial Revolution to deliver on its promise, we must ensure a sense of stability, predictability and trust in cyberspace. These are critical for businesses to prosper, for the health and financial sectors to function, and for national security. For all these reasons cybersecurity must be recognized and promoted as a fundamental public good and I invite students to consider the importance of ethics in cyber-space, including the opportunities and challenges of Artificial Intelligence developments as essential elements in the cybersecurity ecosystem.

Adam Koniuszewski

Fellow of the Quebec Order of Chartered Professional Accountants, Chartered Financial Analyst, Member of the Association of Certified Fraud Examiners, Investor, lecturer, Executive in Residence at Geneva Center for Security Policy (GSCP), Coordinator of the Polish GSCP hub at the Swiss Embassy in Poland, Member of the World Academy of Arts and Science, founder of The Bridge Foundation.

REGIONAL
CYBER LABS

Anna Kowalczyk

Medical University of Warsaw
Faculty of Medicine

RECOMMENDATIONS
HEALTH DOMAIN

Source material collected as part of the curriculum analysis carried out in cooperation with students from eleven Polish medical universities: Medical University of Białystok, Białystok Institute of Cosmetology and Healthcare, Collegium Medicum of M. Copernicus University in Bydgoszcz, Medical University of Gdańsk, Collegium Medicum of Jagiellonian University, Medical University of Łódź, University of Opole, University of Warmia and Mazury, Medical University of Warsaw, Medical University of Wrocław, Collegium Medicum of Zielona Góra University.

Medical school domain executive summary

(pages 29 to 34 in Polish version of the report)

COVID-19 sent shockwaves across global markets reminding us how interconnected healthcare and the economy have become. Alongside the pandemic, law enforcement agencies identified a massive increase in cybercrime. But long before, healthcare was already a preferred target of cyber criminals – a threat for which health facilities and physicians continue to be largely unprepared. Recent months saw an intensification of increasingly sophisticated attacks putting additional strain on healthcare providers already struggling to cope with the pandemic.

Medical students believe in the power of the digital revolution to improve the quality, cost and effectiveness of health services. They are also increasingly aware of the associated cybersecurity challenges. Given the nature of their services and sensitivity of information they handle, security breaches at health facilities can have serious consequences for patients, staff and the institution. But threats are not limited to malware attacks against system integrity and patient privacy. DDoS (distributed denial-of-service) incidents can also impair their ability to operate. Entire hospitals were shut down by attacks leading students to conclude that cyberthreats represent a clear and present danger for public health.

The pandemic invariably accelerated the digitalization of healthcare. Online and telephone consultations replaced many face to face consultations – with benefits and shortcomings. And while deploying telemedicine proved vital for urgent and efficient patient support, the inseparable question of data protection and system integrity was often overlooked opening new vulnerabilities and patient safety issues.

In preparation for this report, medical students were surveyed to determine their familiarity and attitude towards cybersecurity and its inclusion in their study programs. The vast majority was favorable and eager to improve their cyber-knowledge and skills while only 18% touched on the topic in their courses. 90% see a natural fit for including cybersecurity in existing courses, such as Bioinformatics or Medical Law.

Given the rapid and accelerating digitalization of healthcare, medical students consider cybersecurity to be vital element in their professional training and developed recommendations in the following 5 priority areas to be implemented in their curricula:

1 — Real-life examples / cases studies

Real-life examples / cases studies of cyber-incidents give an exciting, realistic and practical approach to illustrate various categories of cyber-threats (WannaCry, data breach, etc.) and possible responses.

RECOMMENDATIONS HEALTH DOMAIN

2 — *Data security*

From the onset and certainly prior to starting clinical internships, health professionals must become familiar with data privacy /HIPAA rules, regulations and best practices - including safeguards from hackers and cybercriminals.

3 — *Best practices for cyber-hygiene*

Health professionals must know how to secure their own profile, accounts, data, passwords, backups, keep their programs updated and to be familiar with popular social engineering techniques, phishing, medical sector scams, as well as ransomware and malware attacks.

4 — *Familiarity with healthcare IT systems*

Medical students should have a general understanding of IT systems used in the sector – including those used in private practices, and must remain current with developments in the sector.

5 — *Military health facilities*

Military health facilities demand a heightened awareness of cybersecurity. Hence, students in military training under the Ministry of Defence should receive additional training in this area.

REPORT CO-AUTHORS HEALTH DOMAIN

Mateusz Guziak — Medical University of Gdańsk, Faculty of Medicine
Nicholas Karolak — Nicolaus Copernicus University in Toruń, Collegium Medicum
Miłosz Korczak — University of Zielona Góra, Collegium Medicum
Julia Makuch — Wrocław Medical University, Faculty of Medicine

Dagmara Gaweł-Dąbrowska, MD, PhD

The need to digitalise Polish healthcare has been widely discussed for over 20 years. In 2000, it seemed this would proceed dynamically. The Centre for Healthcare Information Systems (CSIOZ) was setup at the Ministry of Health to spread the use of IT tools in health facilities. Since its launch, there was talk of an IT system to allow exchanges between patients, medical personnel and insurers. From the onset, security of data storage and transmission was a priority. Despite widespread enthusiasm, these goals were not achieved for lack of legislative solutions, and, as authors rightly note, the human factor.

In 2011, the Health Care Information System Act allowed the development of databases and IT systems at institutions collecting data on medical staff and the services themselves. Data security was entrusted to the Ministry of Health, along with responsibility for online platforms connecting entities in the sector. This increased security of sensitive medical data flows but did not eliminate cybersecurity risks.

The authors call for better cyber awareness by users of IT systems in healthcare, including medical students. The key to success is education. It seems important to involve experts in leverage practical activities and workshops. I fully agree that medical staff should be familiar with the basics of cybersecurity and the safe operation of IT infrastructure in healthcare.

The report also calls for better cybersecurity education in medical universities and I congratulate the authors on their constructive approach and their practical examples to achieve this. This valuable initiative can help step-up medical study programs for the digital era.

Basics that any medical student should be familiar with include tools for creating and storing passwords, securing personal accounts, and familiarity with programs used in patient services. As the ability to share information across entities and systems will soon be a reality, future doctors must have the knowledge and skills to operate safely and effectively in this space.

The challenges and opportunities described are all the more important and urgent because of the accelerating digitalisation of healthcare brought by the pandemic. Knowledge of cybersecurity should therefore not only be part of medicine faculty courses but also in the field of public health education.

Dagmara Gaweł-Dąbrowska

Senior lecturer at the Chair and Department of Social Medicine at Piastów Śląski Medical University in Wrocław, specialist in internal diseases, rheumatology and public health.

LAW & REGULATIONS

REGIONAL
CYBER LABS

Weronika Bańska

President ELSA International
The European Law Students' Association

RECOMMENDATIONS
LAW & REGULATIONS DOMAIN

Source materials were collected as part of the analysis of curricula carried out in cooperation with students from eleven law faculties at the following Polish universities: University of Białystok, University of Gdańsk, Kardynał Stefan Wyszyński University in Warsaw, University of Łódź, Maria Curie-Skłodowska University in Lublin, Nicolaus Copernicus University in Toruń, University of Rzeszów, University of Warsaw, University of Warmia and Mazury in Olsztyn, and the University of Wrocław.

Law school domain executive summary
(pages 37 to 45 in Polish version of the report)

The law profession is known for being conservative and traditional. As lawyers are focused on knowledge and not products, they have so far managed to avoid drastic changes in their practices. There are signs however that the current crisis will be transformational. For starters, just as for physicians, conventional meetings with clients have shifted to remote appointments. A situation unthinkable just a few months ago. This forced lawyers to embrace online meeting software and technologies opening a floodgate of developments from artificial intelligence to machine learning, and including algorithms to price client services.

With clients going digital, lawyers followed. This adoption of new technologies by the legal profession is unprecedented and signals a transformative trend driven by client expectations for faster and better service with squeezed margins. This goes beyond using new tools and systems. The explosion of cybercrime, often cross-border, presents multiple challenges for which an understanding of technological developments and cybersecurity is necessary. To stay ahead, law schools must adapt their content and teaching methods for the digital age for which law students identified the following 6 priority areas:

1 — IT for lawyers

Additional IT courses to help future lawyers maintain proper cyber-hygiene and understand the challenges and opportunities of the digital age for the profession. This includes, but is not limited, to the development of digital tools for law practices, etc.

2 — Cybersecurity Courses

In response to the proliferation of cybercrime, more emphasis, including through dedicated obligatory courses, should be devoted to cybersecurity and its implications. Throughout, interdisciplinarity and cooperation with other fields (business, medicine, IT, etc.) should be emphasized. Specific areas of interest include: coding for lawyers, data analysis, prevention of cybercrime, use of technology in legal proceedings, introduction to cryptology, etc.

3 — Specialization in Cybersecurity

A growing number of students would like to focus on cybersecurity as their specialization and their thesis. This calls for a broader portfolio of courses on technology / cybersecurity and lecturers with relevant expertise.

RECOMMENDATIONS
LAW & REGULATIONS DOMAIN

4 — EU / international regulation

Cross-border cooperation on cybercrime is needed. Lawyers must understand laws across jurisdictions which necessitates specialized courses.

5 — Cybercrime and criminal law

The proliferation of cybercrime, not prevalent when the current penal code was adopted (1997), demands a greater emphasis in criminal law courses.

6 — Wider competencies for lawyers

The digital transformation calls for lawyers to develop news kills. Formal education including mathematics, logical thinking and economics will help students develop strategic vision and critical thinking abilities for the digital age.

REPORT CO-AUTHORS - LAW & REGULATIONS DOMAIN

Natalia Boguszewska — Faculty of Law and Administration, University of Łódź
Zuzanna Choińska — Faculty of Law and Administration, University of Warsaw
Klaudia Jędrzejowska — Faculty of Law and Administration, University of Łódź
Jan Lewit — Faculty of Law and Administration Kardynał S. Wyszyński University in Warsaw
Janusz Linowski — Faculty of Law and Administration, Maria Curie-Skłodowska University
Łukasz Lisowski — Faculty of Law and Administration, University of Łódź
Marcelina Łukowicz — Faculty of Law and Administration, University of Łódź
Mikołaj Niedźwiadek — Faculty of Law and Administration, University of Łódź
Piotr Orzechowski — Faculty of Law and Administration Cardinal S. Wyszyński University in Warsaw
Zuzanna Piątek — Faculty of Law and Administration, University of Łódź
Andrzej Porębski — Faculty of Law and Administration, Jagiellonian University in Cracow
Kacper Stoś — Faculty of Law and Administration, University of Łódź
Filip Strzępek — Faculty of Law and Administration, University of Łódź
Agata Zalewska — Faculty of Law and Administration, University of Warmia and Mazury in Olsztyn

EXPERT OPINION

Kamil Mamak, PhD

It is a truism that new technologies play a crucial role in our lives. It seems that, as a whole, people do not have to be persuaded about this. What appears more troublesome, however, is giving practical expression to this observation. This report is an attempt to demonstrate how technology and its increasing importance influence the education process of prospective lawyers.

It paints a picture of law studies which fail to fully take into consideration the social role of technology, especially in the context of cybersecurity, which was the focal point of interest for students during this project.

Cybersecurity issues are important not only from the point of view of future law school alumni's clients but also from the perspective of the graduates themselves. Law firms as well as judges and prosecutors should be prepared for threats, which are becoming increasingly frequent.

The report presents a considerable degree of maturity in its approach to the issue. This can be seen in the manner in which the authors pay special attention to the need for equipping law students with the ability to understand certain issues independently. Some universities around the world undertake special efforts to meet those expectations by offering coding courses as a part of their law degree program. However, the report also indicates a demand for courses such as Logic and Mathematics.

Furthermore, the authors point to the insufficient number of IT and cybersecurity specialists among the law faculties' staff. It seems that the presence of such experts would enable faster reactions to the ever-changing threats and teaching methods better adapted to the current reality.

It was also noted that courses focusing on crime are lacking in the field of cybercrime education.

The criminal world is dynamic and evolving. Since criminal activity increasingly involves the use of new technologies, this area certainly deserves greater attention. It appears that those responsible for designing law degree curricula should look into this report with great attention, since it contains a plethora of valuable information for positive change.

Kamil Mamak

PhD in Law and Philosophy. Assistant at the Chair of Criminal Law at Jagiellonian University. Board Member of the Krakow Institute of Criminal Law.
Expert on the influence of new technologies on society and criminal law.

DEFENCE

REGIONAL
CYBER LABS

Tomasz Kowalewski, Karol Spychała

General Tadeusz Kościuszko
Military University of Land Forces in Wrocław

CYBERSECURITY IN MILITARY EDUCATION

The specificity of military education restricts the extent to which an evaluation of content and methods of teaching can be shared publicly. For these reasons, recommendations from the military student community, including their views on the implementation of cybersecurity in their curriculum, are not presented here. Still, a general conclusion about the importance of taking into account the overall cybersecurity ecosystem as part of the military student education is detailed below.

Cadets from the following military academies took part in this years' edition of the CyberSecurity Challenge PL2020 tournament: The Polish Naval Academy „Heroes of Westerplatte" Academy in Gdynia (Faculty of Mechanical and Electrical Engineering), and the General Tadeusz Kościuszko Military Academy of Land Forces in Wrocław (Faculty of Security Sciences, Security Engineering and Management).

The interaction between military and civil university students - as part of the multidisciplinary teams of each voivodeship - was considered by cadets as one of the most important educational elements of the simulation. The exercise allowed them to see first-hand the complexity and reach of a cyber-attack including its strategic, regulatory, organizational and telecommunications dimensions and its impact on the state and its critical infrastructure, private enterprise and the lives of millions of Poles.

The inclusion of the multi-faceted and cross-border aspects of cyber-threats helped raise the situational awareness of military students. Still, they could focus their contribution and response on military considerations within a team response that included civilian and military aspects.

The experience acquired in the tournament and its continuation within the regional activities of the Cyber Labs helped broaden the knowledge and competencies of future professional soldiers on the functioning of the cybersecurity ecosystem and on how civilian and military domains complement and reinforce each other.

Our thanks for your interest in the project:

Dariusz Skorupka, Brig Gen, PhD Eng
Rector - Commander
General Tadeusz Kościuszko Military University of Land Forces

Kazimierz Worwa, PhD Eng
Dean, Faculty of Cybernetics, Military University of Technology

Przemysław Rodwald, Cdr PhD Eng
Head of the Department of Computer Systems, Faculty of Computer Science
Polish Naval Academy of the Heroes of Westerplatte

REGIONAL CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland

MODULES

LAW | BUSINESS | INFORMATION TECHNOLOGY | HEALTH | DEFENCE | LOOKING AHEAD

Participation in the project allowed students to engage with university representatives and external stakeholders on shaping the university curricula as it relates to cybersecurity and to constructively contribute to the digital transformation process.

Their recommendations are currently being discussed with the various student authorities. These are an integral part of the campaign to raise awareness about the importance of the digital transformation and cybersecurity in strengthening the university curricula.

Art. 28. 2 from the Act of 20 July 2018 – Law on Higher Education and Science (Journal of Laws 2018, item 1066) reads that "the study program requires consultation with the student council." This means that every university program in Poland is to be co-created with students, through their representatives. In practice, university authorities invite student governments to provide their opinions on study programs. These are prepared on the basis of student government projects and consultations with the student community.

The nationwide promotion of the conclusions in this report has been taking place locally in the Voivodeship Cyber Labs through conferences, roundtables and debates. Activities are prepared by local leaders. It is a space for creating new partnerships and strengthening exchanges between different communities, and a platform for innovation in education on cybersecurity.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

REGIONAL CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland

Alongside formal education, another key element in the process of educating is the so-called informal education within peer groups, mainly carried out with the support of nongovernmental organizations. Combining these two dimensions is important for creating smart specializations that are supportive of social inclusion – a crucial aspect in the digital transformation process. CyberSecurity Challenge PL, the interdisciplinary cybersecurity knowledge competition promotes this cooperation in the field of cybersecurity education. It is an investment based on solid know-how to build trust in the digital economy, a driver of our competitiveness and a common good that serves the greater public interest.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

PIOTR ALBRECHT
Director of Security
Warsaw Stock Exchange

The complexity of the modern economy means that cybersecurity must combine technological, legal and organisational aspects, including the management of information, data, risk and compliance. The interdisciplinarity of cybersecurity and rapid developments in the field must therefore permeate education. It is clear that this calls for ongoing education. Only continuous learning of cyberthreats can be truly effective.

GRAHAM CARR
President and Vice-Chancellor
Concordia University Montreal, Canada

As host of Canada's largest university-based cybersecurity lab, we have seen demand – from students and society – multiply quickly in this rapidly evolving and strategic field. Preparing the next generation through cybersecurity education that combines diverse perspectives and expertise and promotes equitable governance is critical to the future success of our interconnected planet.

FRANCESCO CHIARINI
Director of International Projects
ISSA Poland

The best cybersecurity professionals possess more than expertise on a narrow security domain. The evolution of IT frameworks calls for everyone in information security roles to collaborate. A broader view of legal implications from secure code/configuration, incident response procedures, to writing a policy or standards is now essential. Cybersecurity is more and more about fusing the security concepts into business processes, code and organization response. We need ongoing education to remain the best subject-matter experts and we can't forget to truly partner with our internal and external peers.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

JOLANTA PLIETH-CHOLEWIŃSKA

Department of Strategy, International Cooperation and Public Information
Head Office of Geodesy and Cartography

The importance of cybersecurity became evident during this pandemic with so many activities moving online. This coincides with growing threats in cyberspace. Good information security is no longer enough. Combining the efforts of specialists from many areas is needed to effectively prevent and respond to attacks. One of them is Public Relations – without well-prepared and implemented communication that provides reliable information and education, other cybersecurity measures will remain insufficient.

ALEKSANDER CZARNOWSKI

CEO AVET Information and Network Security

There are few such interdisciplinary fields as cybersecurity. This helps explain why the domain is often misinterpreted. For a good understanding of the subject one needs knowledge in the field of IT, information security theory, cryptography and algorithm design. But also in human sciences including law and business, particularly management and economics. To achieve success in cybersecurity, one must understand the business needs of the and be able to speaks its language to communicate with its IT staff, developers, architects, lawyers, compliance and audit departments, and of course to earn the trust and respect of senior management and the supervisory board.

MARTHA DELGADO

Undersecretary for Multilateral Affairs and Human Rights
Ministry of Foreign Affairs, Mexican Government

Education is crucial given the increasing use of IT by billions so that the opportunities for development are in balance with the protection of fundamental rights and the promotion of peaceful and lawful uses. Education helps increase awareness and choices. IT users have the right to harness its advantages, but also to know the vulnerabilities they face. They must keep up with innovation as there is always something to learn and if knowledge is power in the real world, it is also power in the virtual one. This will become an integral component of education given the need to be digitally alphabetized and functional. Knowledge will always be the best defence against any challenge.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

BRUCE DORRIS, J.D., CFE, CPA

President and CEO, Association of Certified Fraud Examiners

In the wake of COVID-19, cybersecurity education is more important than ever before, as organizations watch cyber fraud risk increase at an accelerated rate. Since information is the currency of the digital age, gaining access to proprietary data is now more valuable than stealing cash. Organizations in all industries increasingly need people trained on the cutting edge of cybersecurity to develop advanced programs to protect their information assets, just as they've done for protecting financial assets in the past. Well-trained cybersecurity experts are a necessary asset to any organization.

WOJCIECH FILIPKOWSKI, PhD, Assoc. Prof.

Laboratory of Criminology, Department of Criminal Law and Ciminology
Faculty of Law, University of Białystok

Investigating cybersecurity, and cybercrime in particular, in a conventional way, i.e. from the point of view of individual knowledge areas, provides a short-sighted picture that will always be incomplete. Those who, in the public or private sector, are active in preventing and combating multidimensional threats in cyberspace must be equipped with competencies that allow an indepth and interdisciplinary investigation. It is therefore well-worth including the possibilities of criminology and forensic science in their education.

COL. MARIUSZ FRĄCZEK, DSc, Assoc. Prof.

Security Branch in Cyberspace
Institute of Safety Engineering, Faculty of Security Studies
General T. Kościuszko, Military University of Land Forces

Cybersecurity education is a priority for our staff and professional soldier candidates, and a pressing concern of the Armed Forces of the Republic of Poland. We are preparing our specialists to face these new challenges and the reallocation of tasks not only for kinetic activities and crisis situations but also in the fifth domain of human functioning and warfare. Building the practical skills of our soldiers is of the greatest importance.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

PIOTR GNYP

Director of Business Development Walkabout Games
Judge in the CSC PL2020 tournament

Our lives have largely shifted to the virtual space. Hygiene in this new dimension should be as important as our personal hygiene. Just as we are trained on what to do in the event of a fire, accident or flood, we also need training on how to react during and after a cyberattack. And, of course, on how to prevent it.

MACIEJ HULICKI, PhD

Head of the „Humans in Cyberspace" and „Security in the Digital Economy" courses
Faculty of Law and Administration, Kardynał S. Wyszyński University in Warsaw

The complexity of problems in the digital world demands comprehensive solutions and coordination. As cybersecurity brings together issues from different domains, education in this field also calls for an interdisciplinary approach. This enables a holistic understanding of these challenges for solutions that can help address the risks associated with digitalisation.

KRZYSZTOF JAJUGA, PhD, DSc, Prof. Tit

Head of the Financial Investments and Risk Management Department
Wrocław University of Economics and Business
President CFA Society Poland

Success in business comes from generating new ideas and the cooperation of interdisciplinary teams that create synergy between their members. A great example is the report on interdisciplinary cybersecurity education. Apart from its undisputed benefits, technological innovation also leads to increased risk and education is needed for effective risk management. The importance of crosscutting knowledge should not be underestimated as it also gives graduates the ability to change careers several times in their life. This would not be possible without interdisciplinary knowledge.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

MICH KABAY, CISSP-ISSMP

Professor of Computer Information Systems
School of Cybersecurity, Data Science & Computing
Norwich University and Military College, Vermont, USA

The increasing integration of information technology into our world has led to parallel increases in the importance of information assurance (IA). Email, chat, video conferences, voice over IP, and social media have greatly increased the opportunities for abuses such as invasion of privacy, bullying, theft of data, and denial of access. The growth of the internet of things includes critical systems controlled by poorly designed, badly implemented software and firmware in industrialprocess controllers and medical devices where bugs and attacks can cause disasters. IA protects everyone!

MARCIN KOBYLIŃSKI, MBA, CISM, CRISC

Chairman of the Auditing Committee ISSA Poland
Judge in the CSC PL2020 tournament

The set of competencies of a „cyber-securer" should cover information technology, higher mathematics, software programming/testing, foreign languages, basic economics, law, psychology/sociology, and issues linked with biometrics. Interdisciplinarity was, is and will remain essential for anyone involved in cybersecurity. A notable example is a nestor of Polish cybersecurity, Colonel Jan Kowalewski. He was famous for breaking Soviet ciphers in 1919/20. He graduated from high school in commerce, studied chemistry at the University of Liège and was fluent in several foreign languages. He did not have a mathematical education, but knew the reality of service in the tsarist communication armies. He had an open, logical and inquisitive mind and a good memory.

HUBERT ŁABĘCKI

Chairman of the Polish Bank Association Business Continuity Group

The shift of modern society activities to cyberspace is changing the nature and singularity of the threats we face. Nowadays, access to information is a key asset - the better we understand this, the faster and more effectively we can prevent, protect and react to existing and future threats. That is why the creation of a conscious society with interdisciplinary knowledge in the field of broadly defined security (including cybersecurity) has become a must.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

DANIEL MCMAHON, FCPA, FCA

Rector Université du Québec à Trois-Rivières, Canada

Digital security raises several issues in academia: the importance of guaranteeing the integrity of our IT infrastructures, preserving the information of members of our community, protecting research data while reconciling ethics and open research, and to train students and our employees. Evolving in a digital age implies precaution and vigilance, but also prevention and education. As our graduates are the leaders of tomorrow, it is our responsibility to help making them enlightened, aware, equipped and able to face current and future challenges including cybersecurity.

GENEVIÈVE MOTTARD, CPA, CA

President and CEO

Order of Chartered Professional Accountants of Quebec

Risk management is at the heart of our profession. With the digitalization of companies in the era of big data, cyber risks represent the pet peeves of many organizations. In this constantly evolving context, cybersecurity is essential for ensuring sound risk management and informed decision-making. Our professionals of tomorrow must know how it works and develop this expertise.

BARTOSZ POSTULKA

Akademia Górniczo-Hutnicza im. S. Staszica w Krakowie

AGH Space Systems

The democratization of space has opened a new horizon for research and innovation. However, new opportunities also reveal new weaknesses in space cybersecurity. Commercial satellites communicate with Earth wirelessly, often using standard TCP and UDP protocols as the transport layer. An interdisciplinary approach to education allows understanding the issue of cybersecurity as a key element of both terrestrial and orbital telecommunications systems. A good example of such an activity is the CyberSecurity Challenge PL2020 as a place to learn and develop for students.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

PIOTR PRZYSTAŁKA, BEng, PhD, DSc, Assoc. Prof.

Deputy Head of the Department of Fundamentals of Machinery Design
Faculty of Mechanical Engineering
Silesian University of Technology

Cybersecurity education for automated systems should use a practical approach with modern tools to support the teaching process. In this respect, industrial process simulators taking into account cyberattack scenarios will play a particularly important role. Due to the lack of commercial simulators with this functionality, members of the AI-METH Scientific Circle designed and built laboratory stations that simulate cyberattacks on industrial control systems. This opens up new learning and research opportunities and lays the ground for additional initiatives related to cyberattack detection and isolation systems.

PRZEMYSŁAW RODWALD, Cdr, PhD, Eng

Head of the Department of Computer Systems, Faculty of Computer Science
Polish Naval Academy of the Heroes of Westerplatte

The Cybersecurity Strategy of the Republic of Poland emphasises the need to develop crosscutting specialisations related to cybersecurity at universities. It is interdisciplinarity, understood as encompassing a combination of ICT, technological, legal, economic, organisational and military aspects, that is key to ensuring security in cyberspace. It must be clear however that this represents an ambitious challenge for the modern education system.

TOMASZ SADOWSKI

Head of the Security Department
Cybersecurity Division, National Bank of Poland
Judge in CSC PL2020 tournament

The CyberSecurity Challenge PL2020 gave participants a real-life experience of how difficult and far-reaching the crisis management process can be. Students from various fields that took part in this innovative project were able to see the problems from different perspectives. Cybersecurity is undoubtedly a global challenge for which a better awareness of cyberthreats has become a necessity.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

RÉMI QUIRION, OC, CQ, PhD, MSRC

Chief Scientist of Québec, Canada
Government of Québec

Digital literacy is a must for all in the 21st century. And the COVID-19 pandemic has demonstrated it more clearly than ever before. In that context, the science of cybersecurity and cybersecurity education should be strongly promoted in universities as well as in our societies.

MAŁGORZATA WEBER

Spokesperson for the Military Property Agency
Judge in the CSC PL2020 tournament

The most difficult challenge in cybersecurity is to keep up with the ever-changing character of threats. That is why it is so important to monitor them continuously. Interdisciplinary education is equally important to raise public awareness and actively prevent attacks. Today's students will soon be joining various companies and institutions. They should be equipped to face these new challenges at the earliest stage in their studies. Armed with broad knowledge and the right tools, they will be ready to tackle the challenges of the cyberworld. Experience in the CSC PL2020 tournament will certainly prove invaluable.

KAZIMIERZ WORWA, BEng, PhD, DSc

Vice-Rector for Education
Military University of Technology

The effective provision of security in cyberspace is a complex and multi-faceted problem that entails organizational, legal, economic and military aspects. This new requirement in the digital age calls for an interdisciplinary approach to cybersecurity education, which from a societal point of view, is characterised by learning that is universal and continuous.

EXPERTS ON THE VALUE OF INTERDISCIPLINARY EDUCATION

ANNA ROMAŃSKA-ZAPAŁA, DSc, Eng
Department of Automatic Control and Information Technology
Faculty of Electrical and Computer Engineering
T. Kościuszko University of Technology in Kraków

Cybersecurity is the foundation for the proper functioning of any system. New technologies and innovative solutions have entered all areas of life. Going forward, the key to success will be to develop cooperation in interdisciplinary teams, where, using the know-how of specialists in various areas, complete, optimal and cyber-safe products and services will be created. This is most easily achieved through appropriate modelling of study programs, enabling cooperation in scientific circles, the implementation of research and projects, and targeted cooperation with industry.

ALBERTO ZUCCONI
Secretary General
World University Consortium

Cybersecurity education is needed since it offers effective tools to protect and promote individual and societal rights and foster the processes needed to achieve sustainability and prosperity.

AMBASSADORS ON THE IMPORTANCE OF CYBERSECURITY EDUCATION

H.E. JÜRG LAUBER

Chairman of the UN Open Ended Working Group on Cybersecurity (OEWG)
Permanent Representative of Switzerland to the UN

In the digital age, technology is developing faster than users' comprehension of its implications. In a more and more interconnected world, cybersecurity education becomes increasingly relevant to all fields of studies and the Regional Cyber Labs are an important initiative to create the necessary awareness. Cybersecurity can only be as strong as its weakest link and I wish the young Ambassadors success in their endeavor.

H.E. LLOYD BRODRICK

Ambassador of Australia to Poland

In an interconnected world dominated by new information technologies, ensuring the stability and security of our digital infrastructure is of fundamental importance. The Australian Government is investing record amounts in our cybersecurity capacities, and we are stepping up cooperation with likeminded partners from government, civil society, and business to address international cybersecurity challenges. Ensuring that we can meet these challenges requires building up the next generation of technical and policy experts, making high-quality cybersecurity education an essential public good.

H.E. JUHA OTTMAN

Ambassador of Finland to Poland

The significance of the digital world for foreign, security and defence policy is growing and will be growing globally. This will require the preparedness not only the governments, but also the whole society. Cybersecurity should be high on the mind of every digital user, and education is the key. For us Finns, the purpose of education is to prepare students for the 21st century and for life-long learning. In 2019 the Worldwide Educating for the Future Index rated Finland as the world leader in teaching skills for the future. Currently, we consider Cyber Security is one of the key future challenges.and develop their potential.

AMBASSADORS ON THE IMPORTANCE OF CYBERSECURITY EDUCATION

H.E. CLEMENTINE SHAKEMBO KAMANGA

Ambassador of the Democratic Republic of the Congo to Poland

We must act to avoid digital chaos in Africa. In the Democratic Republic of the Congo, internet access is a luxury for a segment of the population. Used in the administration and state-institutions, it is not yet prevalent in academia for lack of quality fiber networks. Still, we note abuse, cybercrime and bullying that are obstacles for its use in schools. The Internet should provide a safe space for education. I invite the international community to collaborate and help African students improve their internet use, build their skills and develop their potential.

H.E. ALEXANDER BEN ZVI

Ambassador of Israel to Poland

Israel's cybersecurity eco-system is based on cooperation between public and private sectors and academia. This helps guarantee the security of the Israeli cyberspace, ensuring the protection of both critical military and civilian infrastructures against cybersecurity breaches and attacks. Cyber education is a vital component of this ecosystem. Educating the population to be cyber-aware from a young age, and at the same time training the future generations of cyber experts, is crucial for the security of the country and its citizens.

H.E. EDGARS BONDARS

Ambassador of Latvia to Poland

In today's digital age, cyberspace is an important platform for societal interaction, expression and personal activities. For this environment to be safe and reliable, users of Information and Communication Technologies (ICT) need to be aware of the principles of cyber hygiene in cyberspace. Not only public policies but also cooperation between NGOs and industry is essential to improve ICT users' knowledge and understanding of risks and opportunities in cyberspace.

AMBASSADORS ON THE IMPORTANCE OF CYBERSECURITY EDUCATION

H.E. PAUL SCHMIT

Ambassador of the Grand Duchy of Luxembourg to Poland

For a country building its economic strength on ICT and digitalization, cybersecurity is essential to its economic attractiveness. It is key to creating trust in IT for citizens and business. Luxembourg strongly believes that cybersecurity is a collaborative task, involving governments, companies and individuals. In a digital society cyberskills are the 'new basics' to be included in education. Cybersecurity is empowering people: attackers often target our human weaknesses, triggered easily, if we stay unconscious of cyberrisks and best practices. Awareness raising, training and real-life exercises are a great support to develop individual resilience.

H.E. BOŽENA FORŠTNARIČ BOROJE

Ambassador of the Republic of Slovenia to Poland

In the 21st century, security challenges are moving away from only the traditional, physical understanding of security. Today, challenges to our security are ever present in a sphere dominating everyday life – namely online. COVID-19 pandemic has virtually solidified the ‚new way of everyday activities'. We spend more and more time in a virtual world, using the internet for studying, working and social bonding. With ‚online life' forming such a huge part of people's lives, more attention must be directed towards education on possible threats, how to recognize them and protect ourselves and our children. Increasing resilience to cyber threats must become a common goal.

H.E. JÜRG BURRI

Ambassador of Switzerland to Poland

Switzerland welcomes initiatives such as "Regional Cyber Labs" and the Embassy of Switzerland in Poland is proud to patron it. Poland has abundant IT talent and is a great provider of IT services and cybersecurity. Switzerland emphasizes research, strong legal protection, top-notch security and seamless management of data networks, data centers and security operations centers. We also promote internet governance: Switzerland is a hub for key institutions such as the Internet Governance Forum, the International Telecommunication Union, the ICT4Peace Foundation, the Geneva Centre for Security Policy or the World Economic Forum, which are all active in the field and are actively supported by Switzerland!

AMBASSADORS ON THE IMPORTANCE OF CYBERSECURITY EDUCATION

H.E. STEFAN GULLGREN

Ambassador of the Kingdom of Sweden to Poland

Cybersecurity education is a key component of Sweden's national cybersecurity strategy. With the development and increased use of 5G technology, the flow of information will grow rapidly in our societies. It will open up tremendous opportunities, but also involve certain risks. They can, and should, be mitigated by a combination of measures, including by raising awareness of the need for cybersecurity. Such efforts should include the education of young people and students. That is why we warmly support the initiative of The Bridge Foundation and the Cybersecurity Challenge PL2020. Cybersecurity is an area of great potential for cooperation between Sweden and Poland. We will be stronger by acting together.

H.E. GEORGETTE MOSBACHER

Ambassador of The United States to Poland

As our lives become more digital, new vulnerabilities in our networks and cyberspace have been revealed. We must all increase our cybersecurity knowledge and protect our networks. The United States is constantly investing in and enhancing programs that build our cybersecurity talent pipeline, from primary through postsecondary education. We are partnering with countries around the world – including Poland – to promote cybersecurity best practices through a common vision of an open, interoperable, reliable, and secure Internet that encourages investment and opens new economic markets.

H.E. MARTIN ROGER

Ambassador of Republic of Estonia to Poland

The COVID-19 pandemic has shown the need to adapt to digital tools quickly and effectively to make sure that education is not disrupted. We must ensure that our university students and youth operate safely in the digital world, that they are aware of the risks, and also that they keep the necessary cyber hygiene and have the skillset to cope with cyber threats.

CONCLUSION

The ongoing digital transformation and its growing reach impacts everyone. For our well-being, in micro and macro terms, information security has become a key challenge in the process of universal digitalization.

Education that promotes good behavior and practices should be introduced as early as possible, and certainly in primary schools. However, a more targeted focus on cybersecurity should be in place in secondary and higher education to ensure habits that will lead to lifelong learning.

By concentrating the subject of this report at university level, we are proposing, for the consideration of academia, the implementation of programme changes that give students the knowledge and competencies expected by employers while raising the overall level of cybersecurity at the individual and institutional levels.

From reading the report, there is one conclusion common to all domains. Cybersecurity, as a rule across all fields of study deserves greater attention and academia can do more to keep up with its dynamic evolution to satisfy student needs and market expectations.

Fighting cybercrime is an interdisciplinary challenge that requires cooperation between many domains. We therefore believe it essential to introduce teaching about online security and cyber-hygiene on all fronts.

The recommendations presented herewith are aimed at creating a constructive dialogue leading to practical action. From all the insights collected from university students across Poland, the key priorities selected and presented in this report deserve special attention in the coming years.

Students – co-authors of the report
„A new roadmap for cybersecurity education"

PARTNER STUDENT ORGANIZATIONS

REGIONAL
CYBER LABS

#CyberSecurityEcosystem

10 ECONOMY AND INNOVATION

4.0

elsa

The European Law Students' Association

6 INTERNET OF THINGS

12 DIPLOMACY

ESN

Erasmus Student Network
Poland

13 GOVERNANCE AND ETHICS

16 SPACE COLONISATION

STUDENTS' UNION
OF POLISH UNIVERSITIES
OF TECHNOLOGY

9 DEFENCE

1 SECURITY

IFMSA-Poland

International Federation of Medical Students Associations

7 BIG DATA

2 LAW AND POLICY MAKING

§

Studenckie Forum
Business Centre Club

4 ARTIFICIAL INTELLIGENCE

CYBERCHALLENGES HAVE NO BOUNDARIES

REGIONAL CYBER LABS

#RegionalCyberLabsPL20/21
@CyberPoland

JOIN THE ACTION

THE BRIDGE FOUNDATION

REGIONAL CYBER LABS

BIBLIOGRAPHY

„3-2-1 Backup Rule: The Rule of Thumb to Solve Your Data Loss Problems". Udostępniono 29 lipiec 2020. https://securityboulevard.com/2020/05/3-2-1-backup-rule-the-rule-of-thumb-to-solve-your-data-loss-problems/.

„7 Zasad przetwarzania danych osobowych". Udostępniono 29 lipiec 2020. https://praksyma.pl/7-zasad-przetwarzania-danych-osobowych/.

300RESEARCH. „Efekt zamrożenia. Szansa na radykalną cyfryzację gospodarki", b.d. https://impactcee.com/reaction/2020/wp-content/uploads/2020/06/raport_cyfryzacja_final.pdf.

„2018 NortonLifeLock Cyber Safety Insights Report". NortonLifeLock, 2018. https://www.nortonlifelock.com/us/en/newsroom/press-kits/2018-norton-lifelock-cyber-safety-insights-report/.

Amazon. „Dynamo: Amazon's Highly Available Key-value Store", b.d. https://www.allthingsdistributed.com/files/amazon-dynamo-sosp2007.pdf.

AON Polska. „Zarządzanie ryzykiem i Ubezpieczeniami w Firmach w Polsce- Edycja VI", b.d. https://aoncomauthoring.blob.core.windows.net/aoncom2017media/aon.com/media/poland/publikacje/raport%202019-2020/raport-grms-polska-2019-20.pdf?utm_source=Aoncom.

Bandi, Ajay, Abdelaziz Fellah, i Harish Bondalapati. „Embedding Security Concepts inIntroductory Programming Courses". School of Computer Science and Information SystemsNorthwest Missouri State UniversityMaryville, b.d. https://www.nwmissouri.edu/csis/msacs/PDF/Fall%202019/p78-bandi.pdf.

„Breach Barometer Report: Year in Review". Protenus, 2016.

C. Seacord, Robert. Secure Coding in C and C++ (2nd. ed.). Addison-Wesley Professional, 2013.

CERT NZ. „Guide - Default credentials". Udostępniono 29 lipiec 2020. https://www.cert.govt.nz/it-specialists/guides/default-credentials/.

„CI Security", 02.08. https://www.cisecurity.org.

„CVE - Common Vulnerabilities and Exposures". Udostępniono 29 lipiec 2020. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=default+password.

Czech, Marta. Umowa powierzenia danych osobowych jako instrument ich ochrony (b.d.). https://repozytorium.uwb.edu.pl/jspui/bitstream/11320/8735/1/M_Czech_Umowa_powierzenia_przetwarzania_danych_osobowych.pdf.

„Czym są "dane wrażliwe" i czy PESEL jest "daną wrażliwą"?" Udostępniono 29 lipiec 2020. https://niebezpiecznik.pl/post/czym-sa-dane-wrazliwe-i-czy-pesel-jest-dana-wrazliwa/.

DARKreading. „User-Friendly Cybersecurity: Is a Better UX the Key to a Better Defense?" Udostępniono 29 lipiec 2020. https://www.darkreading.com/edge/theedge/user-friendly-cybersecurity-is-a-better-ux-the-key-to-a-better-defense-/b/d-id/1337699?_mc=rss%5Fx%5Fdrr%5Fedt%5Faud%5Fdr%5Fx%5Fx%2Drss%2Dsimple&page_number=1.

„De Zan, Tommaso & franco, fabio. (2020). Cybersecurity skills development in the EU: The certification of cybersecurity degrees and ENISA's Higher Education Database." Udostępniono 29 lipiec 2020. https://www.researchgate.net/publication/340416935_Cybersecurity_skills_development_in_the_EU_The_certification_of_cybersecurity_degrees_and_ENISA's_Higher_Education_Database.

Deloitte. „«Nowa normalność» dla sektora usług finansowych w Polsce, Europie i Azji". b.d. https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl_FSI_Webinar_odcinek_nr_2_30.04_final.pdf.

„Dyrektywa Parlamentu Europejskiego i Rady (UE) w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa w sieci i systemów informatycznych na terytorium Unii". Parlament Europejski, 6 lipiec 2016. https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/dyrektywa_NIS-1-Dyrektywa-NIS-3.pdf.

EITCA. „Certyfikat EITC/IS/EEIS". Udostępniono 29 lipiec 2020. https://pl.eitca.org/certyfikacja/eitciseeis-gospodarka-elektroniczna-bezpiecze%C5%84stwo-informacji/?v=9b7d173b068d.

„EITCA". Udostępniono 29 lipiec 2020. https://eitca.pl/is.

„Equifax used 'admin' as username and password internally". Udostępniono 29 lipiec 2020. https://securityboulevard.com/2019/10/equifax-used-admin-as-username-and-password-internally/.

Google / Harris Poll. „Online Security Survey", b.d. https://services.google.com/fh/files/blogs/google_security_infographic.pdf.

haveibeenpwned. „haveibeenpwned". Udostępniono 29 lipiec 2020. https://haveibeenpwned.com/.

J. Jiang, i G. Bai. „Evaluation of Causes of Protected Health Information Breaches.", 2019, 179,265.

„Jak chronić swoje dane osobowe?" Udostępniono 29 lipiec 2020. https://uodo.gov.pl/pl/138/1221.

KPMG. „Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych", b.d. https://home.kpmg/content/dam/kpmg/pl/pdf/2020/06/pl-raport-kpmg-barometr-cyberbezpieczenstwa-2020-w-kierunku-rozwiazan-chmurowych.pdf.

„Krajobraz bezpieczeństwa polskiego internetu, Raport roczny 2019 z działalności CERT Polska", 2019. https://www.cert.pl/wp-content/uploads/2020/07/Raport_CP_2019.pdf.

Kruse, Clemens Scott, Benjamin Frederick, Taylor Jacobson, i D. Kyle Monticone. „Cybersecurity in healthcare: A systematic review of modern threats and trends". Technology and Health Care 25, nr 1 (21 luty 2017): 1–10. https://doi.org/10.3233/THC-161263.

Krutz, Daniel & Richards, Thomas. „Cyber security education: why don't we do anything about it?" ACM Inroads, 8(4):5-5, 10.1145/3132217 (2017).

lastline. „Practice what you Preach? 45% of Infosec professionals reuse passwords across multiple accounts, Lastline research says". Udostępniono 29 lipiec 2020. https://www.lastline.com/press/press_release_infosec2018_practice_what_you_preach/.

„Maastricht University". Udostępniono 29 lipiec 2020. https://www.maastrichtuniversity.nl/um-cyber-attack-symposium-%E2%80%93-lessons-learnt.

BIBLIOGRAPHY

Ministerstwo Rozwoju. „Raport Nowy Surowiec - otwarte zasoby danych dla polskiej gospodarki", b.d. https://www.gov.pl/web/rozwoj/raport-nowy-surowiec-otwarte-zasoby-danych-dla-polskiej-gospodarki.

„Navigating GDPR Compliance on AWS", b.d. https://d1.awsstatic.com/whitepapers/compliance/GDPR_Compliance_on_AWS.pdf.

Niebezpiecznik. „Jakie hasła mają Polacy? Wyciek haseł 144 000 użytkowników Autocentrum.pl". Udostępniono 29 lipiec 2020. https://niebezpiecznik.pl/post/wyciek-hasel-144-000-uzytkownikow-autocentrum-pl.

OWASP WebGoat. „Learn the hack - Stop the attack". Udostępniono 29 lipiec 2020. https://owasp.org/www-project-webgoat/.

Kaspersky Lab. „Public WiFi Security". Udostępniono 29 lipiec 2020. https://usa.kaspersky.com/resource-center/preemptive-safety/public-wifi.

„Raport NASK - Cyber Policy AD", b.d. 2019 https://cyberpolicy.nask.pl/wp-content/uploads/2020/05/Raport_CyberbezpieczeństwoAD2019_online.pdf.

„Raport OECD - Measuring the Digital Transformation. A Roadmap for the Future", b.d. https://www.oecd-ilibrary.org/docserver/9789264311992-en.pdf?expires=1591890852&id=id&accname=guest&checksum=C9D41D565730C8FE77EF72FA3A78C46D.

„Raport OECD - The Future of Work. OECD Employment Outlook 2019", b.d. https://www.oecd-ilibrary.org/docserver/9ee00155-en.pdf?expires=1591891492&id=id&accname=guest&checksum=C5553CC9EBF0BF8D8C1514BA3113069C.

„Raport OECD - Trends Shaping Education 2019", b.d. https://www.oecd-ilibrary.org/deliver/trends_edu-2019-en.pdf?itemId=/content/publication/trends_edu-2019-en&mimeType=pdf.

„Raport ONZ - The Age of Digital Interdependence Report of the UN Secretary-General's High-level Panel on Digital Cooperation", b.d. https://digitalcooperation.org/wp-content/uploads/2019/06/DigitalCooperation-report-for-web.pdf.

Regulation (EU) 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 (General Data Protection Regulation), Pub. L. No. 2016/679 (2016). https://eur-lex.europa.eu/eli/reg/2016/679/oj.

Kaspersky Lab. „Research on unsecured Wi-Fi networks across the world". Udostępniono 29 lipiec 2020. https://securelist.com/research-on-unsecured-wi-fi-networks-across-the-world/76733/.

„Share of households with internet access in the European Union (EU28) from 2007 to 2019". Udostępniono 29 lipiec 2020. https://www.statista.com/statistics/377585/household-internet-access-in-eu28/.

Stallings, W. Kryptografia i bezpieczeństwo sieci komputerowych. Gliwice: Helion, 2012.

„Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej", 31 lipiec 2020. https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.

OWASP, Web Security Testing Guide. „Testing for Default Credentials". Udostępniono 29 lipiec 2020. https://owasp.org/www-project-web-security-testing-guide/latest/4-Web_Application_Security_Testing/04-Authentication_Testing/02-Testing_for_Default_Credentials.

„The Radicati Group, INC, Email Statistics Report, 2018-2022". Udostępniono 29 lipiec 2020. https://www.radicati.com/wp/wp-content/uploads/2018/01/Email_Statistics_Report,_2018-2022_Executive_Summary.pdf.

Traynor, Patrick, Kevin Butler, William Enck, Patrick McDaniel, i Kevin Borders. „malnets: large□scale malicious networks via compromised wireless access points". Special Issue: Special Issue on Security in Mobile Wireless Networks 3, nr 2–3 (2010): 102–13.

Uchwała nr 125 Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (2019). http://www.dziennikustaw.gov.pl/M2019000103701.pdf.

Ustawa o ochronie danych osobowych (Dz. U. 2016 r. poz. 922), Pub. L. No. 922 (1997). https://archiwum.giodo.gov.pl/144/id_art/386/j/pl.

Ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, Dz.U. 2018 poz. 1560, Pub. L. No. 1560 (2018). https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/T/D20181560L.pdf.

Verizon. „2020 Data Breach Investigations Report". Udostępniono 29 lipiec 2020. https://enterprise.verizon.com/resources/reports/dbir/.

„W 2019 CERT Polska odnotował więcej cyberuderzeń". Udostępniono 29 lipiec 2020. https://www.telko.in/cert-polska-w-2019-r-odnotowal-wiecej-cyberuderzen.

„What personal data is considered sensitive?" Udostępniono 29 lipiec 2020. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/sensitive-data/what-personal-data-considered-sensitive_en.

Yubico. „2020 State of Password and Authentication Security Behaviors report". Udostępniono 29 lipiec 2020. https://www.yubico.com/blog/yubico-releases-2020-state-of-password-and-authentication-security-behaviors-report/.

The European Digital Strategy, https://ec.europa.eu/digital-single-market/en/content/european-digital-strategy

Rozporządzenie Parlamentu Europejskiego i Rady ustanawiające program Cyfrowa, Europa na lata 2021–2027 https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=COM:2018:434:FIN

Raport NATO, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20190315_sgar2018-en.pdf

TABLE OF CONTENT

The Bridge Foundation is a non-profit organization with United Nations Economic and Social Council special consultative status. Active in Switzerland, Canada and Poland with educational programs that address socio-economic and security challenges.

#CSCPL2020 | @CyberPoland

Contact:
office@thebridge-foundation.org
+41 76 585 78 46
+48 601 214 041

THE BRIDGE
FOUNDATION