# Cybersecurity skills and education in the area of Industry 4.0 and smart manufacturing

**Vasiliki Liagkou**
liagkou@uoi.gr

CONVERGENCE 2023

**30 November 2023 - 1 December 2023**
State of Hessen,Montoyer , Brussels.


Department of Informatics & Telecommunications

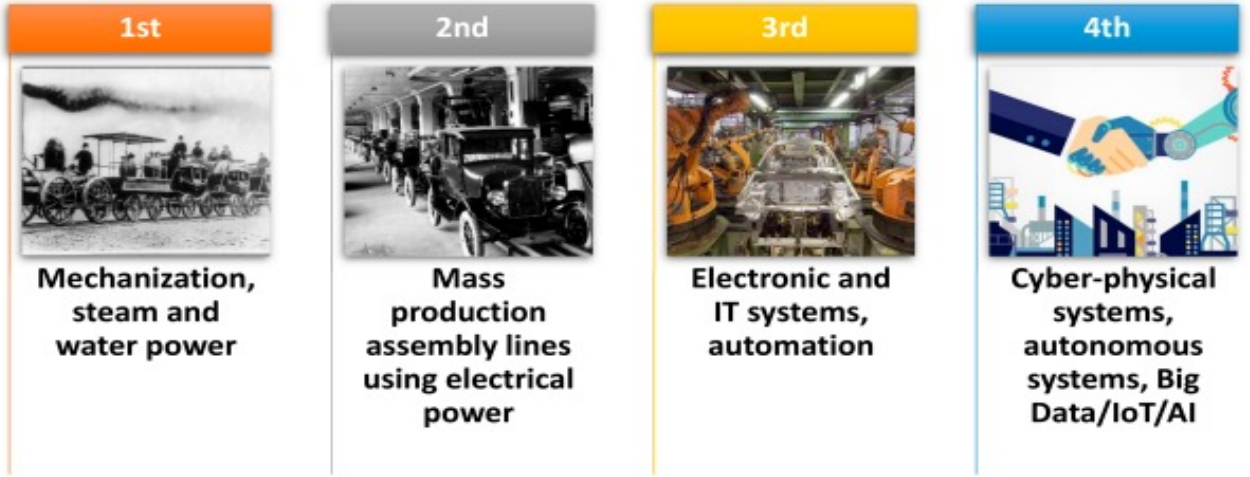
University of Ioannina (UoI)

Arta, Greece

# Introduction


- Industry 4.0 promises revolutionary changes with IoT, AI, and CPS integration.
  - Brings forth intricate cybersecurity challenges that demand meticulous attention.
- Security Landscape Overview
- Educational Gaps: Recognizing a shortage of tailored cybersecurity expertise for Industry 4.0.
  - Barriers posed by the lack of awareness and specialized skills in the workforce.
- Current state of cybersecurity education in the EU
- Bridging the Gap
  - Recommendations to foster cross-functional knowledge, launch targeted training programs, and introduce initiatives at educational institutions.
  - Enisa  & Erasmus+ contribution

# Industry 4.0 Revolution




The four industrial revolutions

- **Evolution of Manufacturing: From Digital to Intelligent Systems"**
  - Introduction to Industry 4.0 (I4.0) and its announcement in Germany in 2011.
  - Transition from digital to intelligent systems.
  - Utilization of high-tech elements: sensors, software, wireless connectivity.
- **Core Principles of I4.0 in Manufacturing"**
  - Principles like smart automation, self-optimization, self-configuration, and self-diagnosis/prognosis.
  - Integration of Machine Learning (ML) and Artificial Intelligence (AI).
  - Real-time data collection and analysis for productivity increase.

# Security Concerns in I4.0

- **Industrial Environment Challenges:**
  - Concern: Industrial systems are not designed for connectivity with the internet
  - Security is a significant barrier for interconnected industrial environments
- **Digital Security in I4.0**
  - Challenge: Safeguarding data in the merger of heterogeneous technologies
  - Reports: Official reports from security companies (e.g., Trend Micro, Kaspersky Lab) on the lack of security in operational industrial interconnected environments

# Main Threat Categories

- **Deception Threats:**
  - Nature: Intentional disruption by industrial competitors or insiders
  - Impact: Causes substantial financial and reputation loss
- **Threats to Industrial Products:**
  - Risk: Unauthorized access impacting product construction
  - Potential Harm: Alteration of products, changes in information
- **Cyberattack Threats:**
  - Challenge: Impact on the heterogeneous architecture of I4.0
  - Examples: Malware infection, unauthorized data modification, and critical data exposure

**Need for validation of Third-Party Code and Software within the industrial context**

- 66% of Attacks Focused on Suppliers' Code
- Customer Assets Targeted: 58% - Predominantly Customer Data, Personally Identifiable Information (PII), and Intellectual Property

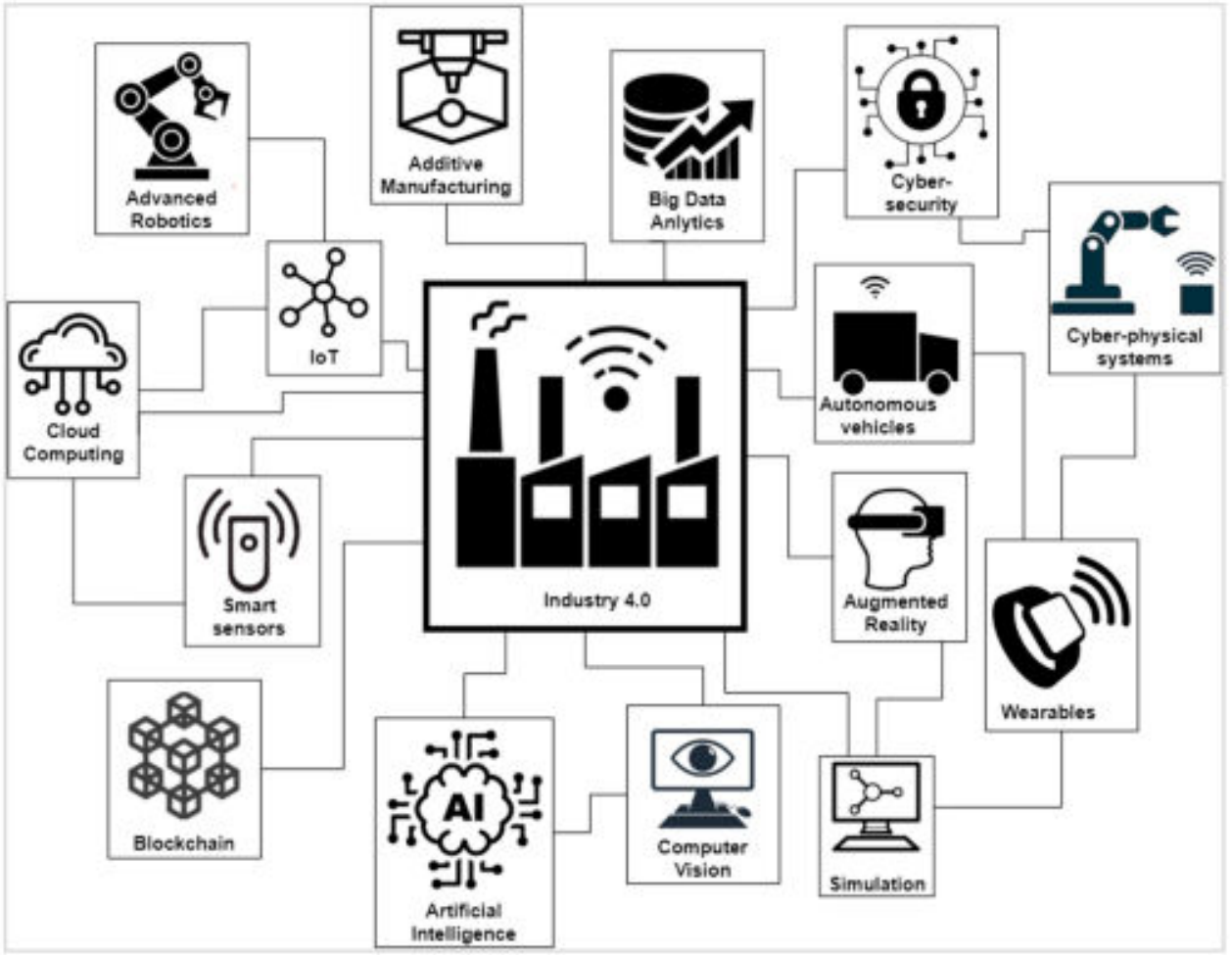
**Maturity Gap in Cybersecurity Incident Reporting Between Suppliers and End-Users**

- 66% of Suppliers Unaware or Failed to Report Compromises
- < 9% of Customers Unaware of How Attacks Occurred

# Security Threats in Main Issues


- **Threats in Operation of I4.0:**
  - Examples: Failure to run requested tasks, holding back planned tasks, financial and reputation loss
  - Risk: Loss of trustworthiness in market relations
- **Threats in Components of I4.0:**
  - Challenges: Malfunction of infrastructure, information systems, parts, stealing or modifying produced data
  - Impact: Loss of trustworthiness in the dynamic environment
- **Threats in Participating Entities:**
  - Concerns: Threatening user's safety, decreasing people's trust
  - Importance: Trust of customers crucial for I.0.4
- **Threats to Economic/Social Relations:**
  - Risk: Impact on relations in the high dynamic, interconnected environment

# Key components of Industry 4.0.




Liagkou, V.; Stylios, C.; Pappa, L.; Petunin, A. Challenges and Opportunities in Industry 4.0 for Mechatronics, Artificial Intelligence and Cybernetics. Electronics 2021, 10, 2001. https://doi.org/10.3390/ electronics10162001

# Threat Landscape in Industry 4.0 Components (1/2)


1. **Cyber-Physical Systems (CPS):**

- IoT-enabled CPS faces internet-based vulnerabilities.
- Real-time sensing, dynamic control, and information services lead to security issues related to confidentiality, integrity, and availability in the product life cycle.

2. **Internet of Things (IoT):**

- Lack of common standardization in IoT components raises security and privacy concerns.
- Questions arise about trusting hardware devices, embedded software, and the reliability of information provided by faulty sensors.
- Interconnected components in the IoT network are susceptible to real-time cyberattacks.

3. **Big Data:**

- Access Control Challenges: crucial for managing production by processing large data volumes.
- Misapplication of global access control may lead to fraud or privacy issues.

# Threat Landscape in Industry 4.0 Components (2/2)


4. **Artificial Intelligence (AI):**

- Autonomous and learning processes raises concerns.
- Threats include modifying learning models or exploiting distributed data for unauthorized output or data extraction.

5. **Cloud Environment:**

- Vulnerable to attacks, including information and service theft through virtualization vulnerabilities.
- Risks to the availability of infrastructure in Industry 4.0 services.

6. **VR/AR Environments:**

- VR/AR applications may not realistically simulate real-life events.
- Malicious users may exploit this limitation to make incorrect decisions and inappropriate actions.

7. **Digital Twin:**

- Digital twin's bidirectional interfaces expand attacker capabilities.
- Hackers gaining control of the digital twin can identify vulnerable attack points, spoof behaviors, or even access the physical system.

# Categorization of Reported Threats Events in I4.0.

| Security Property | | | Component of I.0.4 | Threat Category | Threat Event |
|---|---|---|---|---|---|
| *Confidentiality* | *Integrity* | Availability | - | - | - |
| - | x | - | CPS, IoT, Cloud | Threats in operation of I.4.0 | Countries use cyber threats for controlling production lines |
| - | x | x | CPS, IoT, Cloud | Threats in operation of I.4.0 | NotPetya attack |
| - | x | x | CPS, IoT, Cloud, VR/AR | Threats in operation of I.4.0 | Energy sector Attack |
| x | - | - | CPS, IoT, Cloud | Threats in components of I.4.0 | Hacking service providers |
| x | x | - | CPS, IoT, Cloud | Threats in participating entities | SW hijacked for installing backdoors |
| x | x | - | CPS, IoT, Cloud | Threats in participating entities | Online credit card skimming attack |
| x | - | - | IoT | Threats in participating entities | Harvesting data via SDK |
| x | - | - | CPS | Threats in components of I.4.0 | Compromise S/W for harvesting Data |
| x | - | - | CPS | Threats in components of I.4.0 | Compromise S/W in industrial control systems |
| - | x | x | CPS | Threats in operation of I.4.0 | Exploiting insecure SCADA systems |
| x | - | - | - | Threats in participating entities | Compromised employees |
| - | x | | CPS, IoT, Cloud | Threats in components of I.4.0 | Antwerp port smuggling |
| - | | x | CPS | Threats in components of I.4.0 | Eli Lilly warehouse theft |
| - | x | - | CPS, IoT | Threats in participating entities | Contamination of meat products |
| - | x | x | - | Threats in participating entities | Explosive printer cartridges |

Liagkou, V.; Stylios, C.; Pappa, L.; Petunin, A. Challenges and Opportunities in Industry 4.0 for Mechatronics, Artificial Intelligence and Cybernetics. Electronics 2021, 10, 2001. https://doi.org/10.3390/ electronics10162001

# Critical Cyber Threats Impacting Industry 4.0 (1/5)

CONVERGENCE 2023
CONVERGENCE 2023
30 November 2023 – 1 December 2023
Conferences

**NSA Compromising Encryption Mechanisms**

- NSA accused of compromising encryption mechanisms belonging to security vendors.
- Allegations of inserting backdoors into final products.

**Chinese Attempt to Modify Lenovo Motherboards**

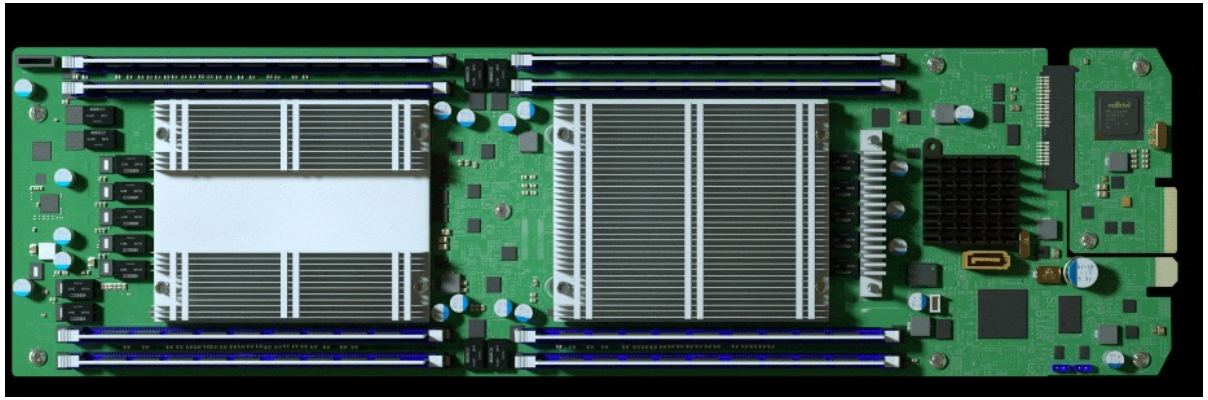
- China attempted to modify Lenovo motherboards' production line to infect them with malicious software.

**Russian Injection of Malware via Legitimate Software Component**

- Russia accused of injecting malware via a legitimate software component.

**Chinese Espionage on Technology Service Providers**

- Chinese spies attempted to steal private information by hacking eight of the world’s biggest technology service providers.



**The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies**

# Critical Cyber Threats Impacting Industry 4.0 (2/5)


**Energy Sector Attacks:**

- Dragonfly, a hacking group, targeted the energy sector in Europe and North America.
- Attempted to disrupt affected operations severely.
- Trojan insertion impacting operational actions
- The group has been in operation since at least 2011


**Global NoPetya Cyber-Attack (2017):**

- Impacted thousands of computers in dozens of countries.
- Exploited a vulnerability in typical software used by Ukrainian companies.
- Resulted in disruptions to shipping, businesses, and a total economic loss of over $10


**ShadowPad and ShadowHammer Attacks:**

- Integrated malicious code into ASUS Live Update Utility components.
- Attackers installed backdoors on millions of devices, connecting them to predefined targets.

# Critical Cyber Threats Impacting Industry 4.0 (3/5)



**Skimming code incidents**

- In 2019, a skimming code was injected into the shared JavaScript libraries of the e-commerce PrismWeb platform, impacting 201 online university campus stores in the US and Canada.
- That same year, Trend Micro also detected and blocked another malicious skimming code loaded on 277 e-commerce websites.
- Designed to infect the JavaScript library belonging to a French online advertising company called Adverline (serving as a "third-party" entity).


- In both incidents, the malicious codes aimed to steal payment data and later send this information to one or several remote servers.
- On April 14, 2019 the attackers injected a script into the payment checkout libraries used by the PrismWeb platform.
- The notorious online credit card skimming attack is known as **Magecart**. The attack, facilitated by a new cybercrime group, impacted 201 online campus stores in the United States and Canada.

# Critical Cyber Threats Impacting Industry 4.0 (4/5)


**Piriform Ltd. Software Attack (2017):**

- Hackers broke into Piriform Ltd.'s free software, potentially controlling millions of devices.
- Targeted recollecting information and gaining access, capabilities, and resources.

**Android Applications Data Harvesting:**

- A group of Android applications harvested contact information on mobile phones without user consent.
- The data-stealing logic hid inside a data analytics software development kit.

**Industrial Control Systems Compromise (2014):**

- Russian group Black Ghost Knifefish compromised software produced by industrial control systems equipment providers in Germany, Switzerland, and Belgium.
- Aimed to extend malware and compromise victims throughout Europe.

# Critical Cyber Threats Impacting Industry 4.0 (5/5)


**SCADA Environment Cyberattack (2018):**

- Exploiting vulnerabilities in third-party systems in supervisory control and data acquisition (SCADA) environments.
- Successfully shut down numerous pipeline communication networks.

**Compromise of Wipro Employees (2016)**

- Three Wipro employees in Kolkata were arrested in connection with a security breach in the customer records of UK-based telecom client TalkTalk.
- Significant implications for the IT company.

**Attacks on Physical Infrastructures:**

- Attacks in port facilities in Antwerp (Belgium) and the Eli Lilly warehouse targeted physical infrastructures.
- Attempts to root or steal products and modify control standards of the production line.

**Explosive Material on Cargo Plane (2010)**

- Explosive material camouflaged through printer cartridges was found on a cargo plane at East Midlands Airport.

# Addressing the Need for Cybersecurity Education in Industry 4.0


## Challenges in Security Expertise

- **Barrier to Adoption:**
  - Issue: Lack of sufficient information security expertise acts as a hindrance to Industry 4.0 security measures adoption.
  - Challenge: Deployment personnel often possess knowledge limited to either IT or OT security, lacking expertise in crucial areas like network security, embedded systems, and the convergence of OT and IT security.

## Adaptation in Traditional OT Environments

- **Introduction of New Technologies:**
  - Change: Industry 4.0 introduces new technologies into traditional OT environments.
  - Need for Adaptation: Employees familiar with OT need to adapt to embrace Industry 4.0 capabilities, requiring new competencies.
  - Lack of Competences: Employees lack essential competences, including operational security skills, understanding new Industry 4.0 protocols, utilizing security functionalities, integrating with legacy systems securely, and managing information systems security in complex supply chains.

# Recommendations Index



**INDUSTRY 4.0 SECURITY EXPERTS (OT AND IT SECURITY)**

- Promote cross-functional knowledge on IT and OT security
- Secure supply chain management processes
- Establish Industry 4.0 baselines for security interoperability
- Apply technical measures to ensure Industry 4.0 security

**INDUSTRY 4.0 OPERATORS (SOLUTION PROVIDERS & MANUFACTURERS)**

- Promote cross-functional knowledge on IT and OT security
- Clarify liability among Industry 4.0 actors
- Foster economic and administrative incentives for Industry 4.0 security
- Secure supply chain management processes
- Establish Industry 4.0 baselines for security interoperability
- Apply technical measures to ensure Industry 4.0 security

**REGULATORS**

- Clarify liability among Industry 4.0 actors
- Foster economic and administrative incentives for Industry 4.0 security
- Harmonize efforts on Industry 4.0 security standards
- Establish Industry 4.0 baselines for security interoperability

**STANDARDISATION COMMUNITY**

- Harmonize efforts on Industry 4.0 security standards
- Establish Industry 4.0 baselines for security interoperability

**ACADEMIA AND R&D BODIES**

- Promote cross-functional knowledge on IT and OT security
- Establish Industry 4.0 baselines for security interoperability

"Industry 4.0 - Cybersecurity Challenges and Recommendations", European Union Agency for Network and Information Security (ENISA), 2019

# Recommendations for Addressing Cybersecurity Education Needs



- **Comprehensive Training Programs:**
  - Proposal: Develop comprehensive training programs covering IT/OT convergence, Industry 4.0 systems, and crucial cybersecurity aspects.
- **Tailored Industry-Specific Training:**
  - Recommendation: Tailor training programs to meet specific industry needs for relevance and effectiveness.
- **Accessible and Cost-Effective Training:**
  - Proposal: Create accessible and cost-effective training solutions to bridge the competence gap.
- **Promote Continuous Learning:**
  - Recommendation: Encourage continuous learning to keep employees updated on evolving cybersecurity challenges and solutions.

# Enhancing Industry 4.0 Security Awareness and Expertise


1. **Intra-Organizational Knowledge Cultivation:**
   - Encourage security personnel within Industry 4.0 organizations to invest in cutting-edge, dedicated cybersecurity training.
   - Emphasize coverage of all essential aspects related to IT/OT convergence and Smart manufacturing in the training programs.
2. **Education at Academic Institutions:**
   - Advocate for specialized training and courses in schools and universities, localized to reach a broader audience.
   - Stress the long-term benefits of promoting Industry 4.0 security understanding among younger generations.

# Recommendations for Cross-Functional Knowledge


1. **Cross-Functional Exchange:**
   - Promote cross-functional security and safety knowledge exchange between IT and OT experts.
2. **Tailored Training Courses:**
   - Launch security education and training tailored for industries transitioning to Industry 4.0.
   - Focus on imparting knowledge about state-of-the-art practices, methodologies, and tools for secure IT/OT convergence.
3. **Competency Profiles Development:**
   - Develop competency profiles to provide IoT and Industry 4.0 specific awareness and education training for all staff members.
4. **Next-Generation Empowerment:**
   - Introduce programs at schools and universities to address the lack of security and safety knowledge across the industry.
   - Empower the next generation of IT and OT security experts through targeted educational initiatives.

# EU Organisations and Partners in Cybersecurity Skills Development


1. **ENISA: EU Agency for Cybersecurity**
2. **European Cybersecurity Competence Centre (ECCC)**
3. **European Cyber Security Organisation (ECSO)**
4. **Council of European Professional Informatics Societies (CEPIS)**
5. **EU-Level Cooperation**

- **Collaborative efforts with international organizations:**
  - UN, OSCE, NATO, OECD, Europol, and others.
  - Global Forum of Cyber Expertise (GFCE).

# Need for increasing awareness and training of cyber security

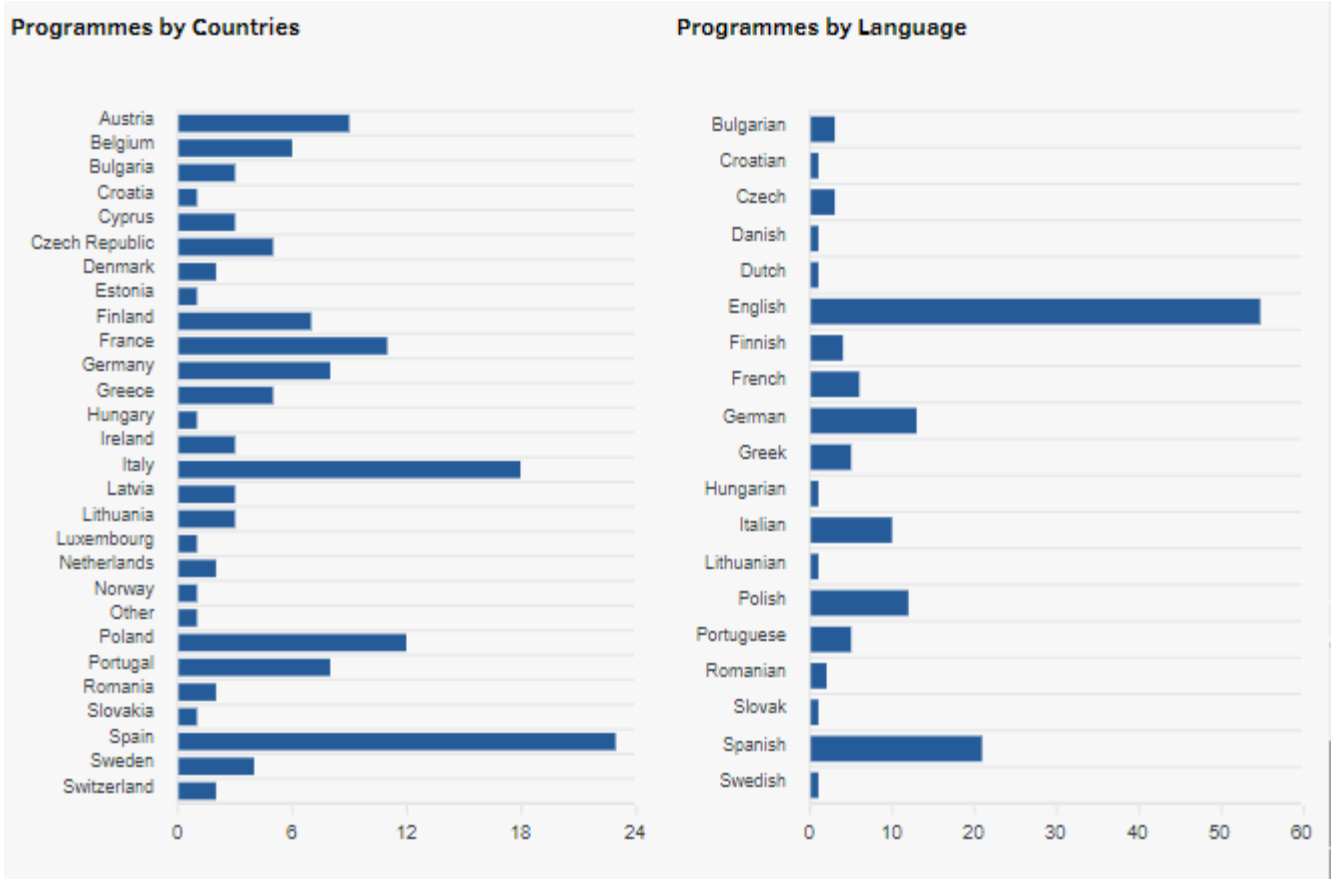

- The 2023 Data Breach Investigations Report from Verizon found that 74% of breaches involved the human element and a staggering 95% of cybersecurity issues were traced back to human error in 2022.
- By incorporating effective cyber security awareness and training programs, organizations significantly protect themselves from a wide range of cyber threats.
- **EU-Level Collaboration**
  - Advocate for coordinated actions and implement good practices at the EU level.
  - Encourage Member States to develop similar capabilities to achieve a unified and robust security posture.
- **ENISA** plays a crucial role in building cybersecurity capacities across the EU. It provides resources, knowledge, and support to enhance the overall cybersecurity posture
- **Erasmus+** contributes to addressing the cybersecurity skills gap by supporting education and training initiatives, and funding programs that enhance the knowledge and skills of individuals in the field of cybersecurity.

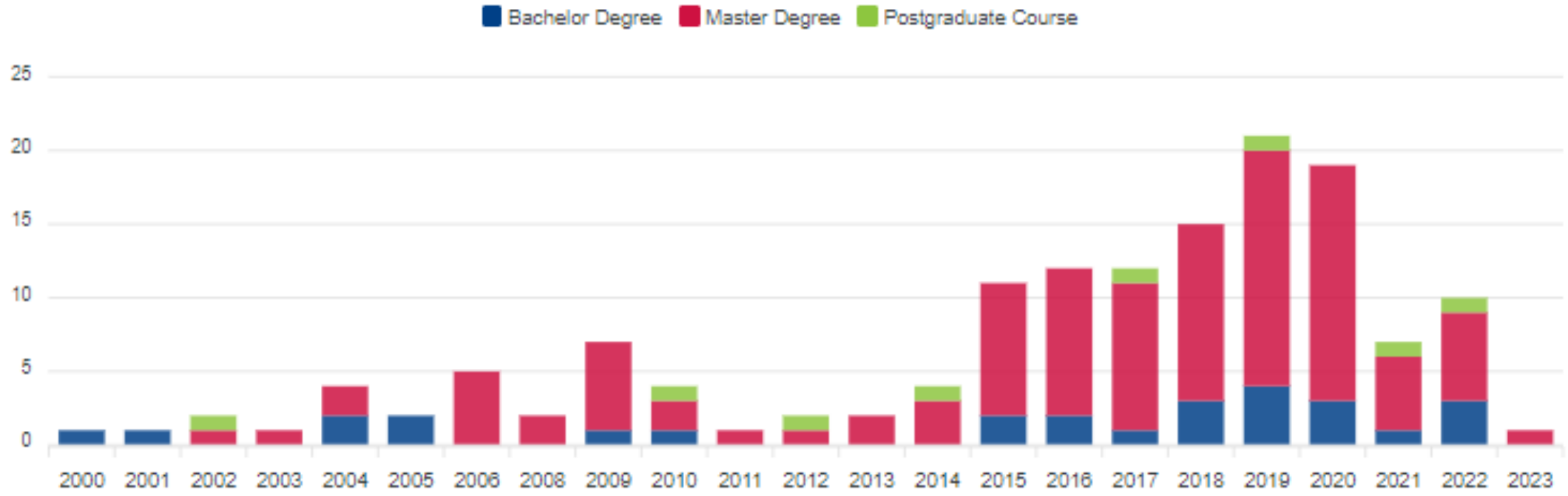
https://www.verizon.com/business/resources/reports/dbir/2023/master-guide/

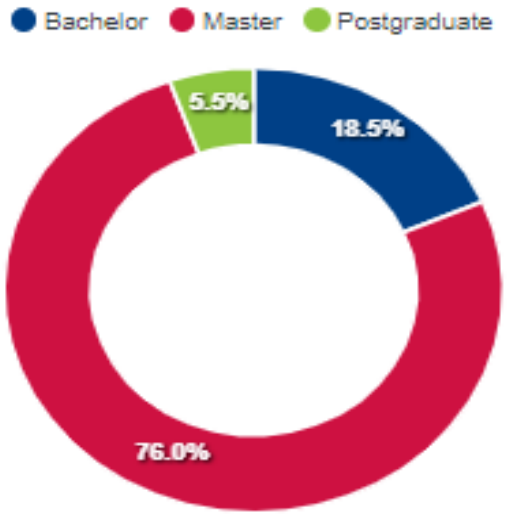
# Understanding the Current State of Cybersecurity Education in the EU


- Problem Statement: Analyzing the supply of cybersecurity qualifications and skills within the EU reveals challenges in the existing educational landscape.
- The insights are drawn from ENISA's Cybersecurity Higher Education Database (CyberHEAD), providing a snapshot of cybersecurity programs in the EU.
  - Limitations in coverage exist, as the database is crowd-sourced and relies on Higher Education Institutions (HEIs) for submissions.
  - CyberHEAD inclusion criteria demand recognition by the national authority of an EU or European Free Trade Association (EFTA) Member State and a significant focus on cybersecurity topics within the degree content

# Understanding the Current State of Cybersecurity Education in the EU


Bachelor Degree
Master Degree
Postgraduate Course
25
20
15
10
5
0
2000
2001
2002
2003
2004
2005
2006
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023


Bachelor
Master
Postgraduate
5.5%
18.5%
76.0%

# Erasmus+


- Erasmus+ is a flagship European Union program that has been in operation for several decades.
- Its primary goals include enhancing education, training, youth, and sports in Europe.
- We'll explore its various components and the impact it has on skills and education.

# Erasmus+ Contribution to Cybersecurity Education and Skills


- Holistic Approach: Fosters collaboration among institutions, industry, and policymakers.
- International Perspective: Enables cross-border exchanges for diverse cybersecurity exposure.
- Innovative Partnerships: Encourages collaborations to keep curricula relevant.
- Skill Enrichment: Supports projects emphasizing practical, hands-on experiences.
- Cultivating Talent: Nurtures the next generation of skilled cybersecurity experts.
- Policy Impact: Contributes insights to shape policies addressing dynamic cybersecurity challenges.
- Continual Improvement: Emphasizes continual adaptation to stay ahead in a rapidly evolving digital landscape.

# EU projects on Cybersecurity


## Completed Projects on Cybersecurity in Higher Education 2015-2020

### Awareness

- Innovative postgraduate programme: Addressing market needs and pioneering new delivery modes
- Manufacturing Education for a Sustainable fourth Industrial Revolution
- Meeting Industrial Demand for Skills in Information Security Education.
- Cyber Aware Students for Public Administrations
- Cybersecurity Curricula Recommendations for Smart Grids
- promotINg Cyber-hygIene in eDucation through sEcuring distaNCe lEarning
- Weeks of International Teaching - Inclusive and Digital
- Collaborative Cybersecurity Awareness Learning
- Cyber Aware Students for Public Administrations
- Digital Competences for Improving Security and Defence Education
- Cyber Security for Psychology

# EU projects on Cybersecurity


## Completed Projects on Cybersecurity in Higher Education 2015-2020

### Training

- An Innovative Higher Education Institution Training Toolbox to EffeCtively AddRess the EUropean InduStry 4.0 Skills Gap and Mismatches
- Cybersecurity fundamentals
- Competence Development in Collaborative Industrial Internet of Things
- Digital Competences for Improving Security and Defence Education
- ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector
- Alliance for developing, teaching and training Digital Forensics and Incident Response students and practitioners
- Digital Training for Cybersecurity Students in Industrial Fields
- Safeguarding against Phishing in the age of 4 Industrial Revolution
- Innovation and Excellence in Cyber-security teaching in Higher Education
- Interdisciplinary training on EU security, resilience and sustainability
- Cyber Security – Training Students and Scholars for the Challenges of Information and Communication Technologies in Research and Studies for Internationalisation

# EU projects on Cybersecurity


## Projects with Results on Cybersecurity in Higher Education 2015-2020

### Awareness

- Cybersecurity Curricula Recommendations for Smart Grids
- Manufacturing Education for a Sustainable fourth Industrial Revolution
- promotINg Cyber-hygIene in eDucation through sEcuring distaNCe lEarning awareness
- Cybersecurity fundamentals
- Meeting Industrial Demand for Skills in Information Security Education
- Innovative postgraduate programme: Addressing market needs and pioneering new delivery modes awareness

### Training

- An Innovative Higher Education Institution Training Toolbox to EffeCtively AddRess the EUropean InduStry 4.0 Skills Gap and Mismatches
- ECQA Certified Cybersecurity Engineer and Manager – Automotive Sector
- Digital Training for Cybersecurity Students in Industrial Fields
- Safeguarding against Phishing in the age of 4 Industrial Reolution

# EU projects on Cybersecurity


## Ongoing Projects on Cybersecurity in Higher Education 2019-2022

### Training

- Cybersecurity in practice for non IT oriented HE courses
- Generation Blockchain
- DIGITAL TRAININIG TOOLS IN STEEL STRUCTURE INTEGRITY
- Príprava budúcich IT profesionálov pre oblasť umelej inteligencie
- Rethinking Cybersecurity in Pakistan - Human factors' Essential Role
- Skill Training Alliance For the Future European Rail System
- European law Perspectives on Innovation Challenges
- Alliance for Strategic Skills addressing Emerging Technologies in Defence
- smartAInnovators: PROMOTING AI-DRIVEN DIGITAL TRANSFORMATION AND INNOVATION IN VET SCHOOLS FOR SOCIAL CHANGE AND BETTER SKILLS MATCH WITH THE LABOUR MARKET
- Cybersecurity Skills Alliance - A New Vision for Europe
- Cyber Security Training on Operational Technology Resilience
- CI: Karriere-Intelligenz
- Micro-Entreprise-Cyber-Security
- Enhancing Cyber Security - Development of trainings using "Escape Room" Model
- Digital Diplomacy: Building the Common Future with Technology

### Awareness

- CyberSecurity for VET and SMEs

# Erasmus in Higher Education


## Students

- Expose students to diverse perspectives, knowledge, teaching, and work practices in the European and international context.
- Develop students' transversal skills (e.g., communication, critical thinking, intercultural skills).
- Enhance forward-looking skills, including digital and green competencies.
- Facilitate personal development, adaptability, and self-confidence.

## Staff

- Enable staff, including those from enterprises, to teach or train abroad.
- Share expertise, gain new pedagogical and digital skills.
- Foster collaboration, exchange best practices, and enhance cooperation.
- Better prepare students for the world of work.

## Transactional Curricula

- Promote transdisciplinary curricula and innovative teaching methods.
- Encourage online collaboration, research-based learning, and challenge-based approaches.
- Aim to address societal challenges effectively.

# Conclusions


- Educational Insights: Examining EU cybersecurity education illuminates strengths and challenges, reflecting the dynamic nature of Industry 4.0 requirements.
- Workforce Alignment: Bridging cybersecurity skill gaps demands targeted actions. Cross-functional knowledge exchange, tailored training, and competency profiling emerge as crucial strategies.
- Long-Term Commitment: From educational institutions to industry leaders, fostering a cybersecurity-conscious culture is pivotal for Industry 4.0's sustained resilience.
- Collaborative Imperative: A united front involving industry, education, and policymakers is essential for creating a robust cybersecurity environment aligned with evolving Industry 4.0 demands.
- Forward Momentum: Prioritizing cybersecurity education and fostering collaboration are essential steps toward a secure and sustainable Industry 4.0 future.