Upskilling and Reskilling Critical Infrastructure Protection Professionals: Learning Paths for 15 Important Skills Profiles

John Soldatos (INNOV-ACTS Limited)

Marianna Charalambous (INNOV-ACTS Limited)

Rauno Pirinen (Laurea University of Applied Sciences)

Version 1.0

1. Purpose and Scope

The European Commission emphasizes the growing need for cybersecurity professionals in Europe. Specifically, an analysis published in 2023 highlighted a shortage of skilled workers, which is estimated at 1 million in Europe and 3.4 million globally [EC23a]. In 2022, the shortage of cybersecurity professionals in the EU ranged between 260,000 and 500,000. The EU's cybersecurity workforce needs were estimated at 883,000 professionals [EC23b].

According to the analysis in [EC23a], the demand for cybersecurity skills is rising, especially following the COVID-19 pandemic outbreak which led to a proliferation of digital infrastructures and digital activities within modern industrial organizations. Moreover, the same analysis report highlights a significant gender disparity, with women comprising less than 25% of the cybersecurity workforce. Furthermore, it underscores the importance of educational initiatives and frameworks to bridge the skills gap, while at the same time enhancing cybersecurity training and workforce diversity. This requires the establishment of comprehensive training programs and inclusive policies, which will equip more individuals with the required cybersecurity competencies. This approach is destined to fill the proclaimed deficit of skilled professionals, but also to foster a more diverse workforce.

The World Economic Forum has also identified upskilling and reskilling as critical drivers for the future of jobs, emphasizing that the 2020s will be pivotal for workforce development. Employers are encouraged to invest in these areas as a significant number of workers' skills will be disrupted within the next few years. This focus is not only essential for individual career resilience but also for maintaining competitive economies in a technologically advancing world[1].

The rapid evolution of threats to critical infrastructure necessitates continuous upskilling and reskilling of professionals in the field of Critical Infrastructure Protection and Resilience (CIP/CIR). In today's fast-paced technological landscape, the complexity and frequency of these threats are on

[1] World Economic Forum (2024) 'The 2020s will be a decade of upskilling: Employers should take notice', *World Economic Forum*, 5 January. Available at: https://www.weforum.org/agenda/2024/01/the-2020s-will-be-a-decade-of-upskilling-employers-should-take-notice/ (Accessed: 12 May 2024).

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

the rise, making it imperative for CIP/CIR professionals to remain at the forefront of the latest advancements and methodologies.

Other recent market analysis reports also underscore this urgency, revealing that nearly 60% of organizations recognize the skills gap in their cybersecurity teams as a significant risk factor[2]. This is particularly concerning given that the estimated cost of cybercrime is projected to reach $10.5 trillion annually by 2025. This staggering figure highlights the escalating consequences of cyber threats and further emphasizes the importance of investing in cybersecurity education and training. Additionally, the challenge of retaining skilled cybersecurity professionals continues to appear intensified. About 60% of organizations report difficulty in retaining qualified cybersecurity professionals, which underlines the need for robust upskilling and reskilling initiatives to maintain a proper cybersecurity workforce[3].

In this landscape, the introduction of new technologies such as artificial intelligence, machine learning, and the Internet of Things (IoT) is continually broadening the scope of potential vulnerabilities. These developments require CIP/CIR professionals not only to master new tools and technologies but also to adopt a proactive approach to threat detection and response. Consequently, upskilling and reskilling becomes a strategic imperative for organizations aiming to safeguard their critical infrastructure.

This goal of the present whitepaper is to present a series of tailored learning paths that can guide learners towards acquiring specific CIP/CIR skill profiles, while facilitating training organizations and human resources departments of critical infrastructure operators to structure relevant training activities. The presented learning paths are designed not only to bridge the current skills gap but also to foster innovation in CIP/CIR practices. Specifically, whitepaper highlights skills profiles and learning paths that support novel security roles in the contemporary CIP/CIR landscape. Moreover, it highlights the need for holistic educational approach that integrates technical, non-technical, and soft skills towards reskilling and upskilling professionals that can cope with modern CIP/CIR challenges.

[2] ISACA (2023) 'New ISACA research: 59 percent of cybersecurity teams are understaffed', *ISACA*, 25 April. Available at: https://www.isaca.org/about-us/newsroom/press-releases/2023/new-isaca-research-59-percent-of-cybersecurity-teams-are-understaffed (Accessed: 12 May 2024).

[3] Scale Venture Partners (2023) *Scale Security Report 2023*. Available at: https://www.scalevp.com/wp-content/uploads/2023/10/Scale-Security-Report-2023-Final.pdf (Accessed: 12 May 2024).

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

2. Skills Profiles and Learning Paths Construction Methodology

2.1. Skills Profiles Identification

The methodology employed for the development of the presented learning paths was driven by the CIP/CIR capability gaps that have been identified in the scope of the EU-CIP project. This first step of our methodology involved analysing these capability gaps towards identifying the professionals' capabilities and skills profiles required to fill them. Each of the identified skills profiles highlights the skillsets that are required to cope with the identified gaps such as gaps in the areas of cyber-physical threat intelligence and emergency response. Given that the capability gaps have been identified by CI practitioners and experts, the presented approach provided a sound basis for aligning educational outcomes with industry requirements. This alignment will be further audited by soliciting feedback from relevant stakeholders (e.g., CI experts, human resources professionals, cybersecurity education experts) following the public release of the present paper. Specifically, EU-CIP will solicit experts' feedback about the relevance of the identified skills profiles and their alignment to CIP/CIR stakeholders' training needs.

The table below showcases the skills profiles identified and a short summary of their respective skills:

Cybersecurity Specialist	The learning path for a Cybersecurity Specialist starts with basic cybersecurity courses and progresses through specialized training in encryption methods, vulnerability assessments, and incident response.
Risk Management Analyst	A Risk Management Analyst's path focuses on courses in risk assessment methodologies, developing risk management strategies, and enhancing communication skills to effectively convey risk information.
Emergency Response Coordinator	The learning path for an Emergency Response Coordinator includes training in emergency management protocols, effective communication during crises, and familiarity with incident command systems.
Physical Security Specialist	A Physical Security Specialist's path covers courses in designing and implementing physical security measures, understanding access control and surveillance technologies, and developing security policies and procedures.
Network Infrastructure Engineer	The learning path for a Network Infrastructure Engineer entails courses in network design and maintenance, network protocols and technologies, and network security principles.
Critical Infrastructure Resilience Planner	A Critical Infrastructure Resilience Planner's path focuses on developing resilience plans, understanding resilience frameworks, conducting risk assessments, and applying strong analytical skills.
Incident Response Manager	The learning path for an Incident Response Manager includes managing incident response teams, developing incident response plans, forensic analysis, and coordination with law enforcement.
Compliance Auditor	A Compliance Auditor's path would focus on courses in auditing, understanding regulatory frameworks, compliance assessments, and developing strong analytical skills.
Industrial Control Systems (ICS) Engineer	The learning path for an ICS Engineer covers designing and maintaining industrial control systems, understanding SCADA systems, and assessing cyber threats targeting ICS.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Crisis Communication Specialist	A Crisis Communication Specialist's path involves developing crisis communication plans, managing communication channels during emergencies, and crafting clear messages for various stakeholders.
Business Continuity Planner	The learning path for a Business Continuity Planner includes developing business continuity plans, understanding continuity frameworks, identifying critical business functions, and conducting continuity exercises.
Data Privacy Officer	A Data Privacy Officer's path would focus on ensuring compliance with data privacy regulations, understanding data protection laws, assessing data privacy risks, and managing data breach incidents.
Physical Infrastructure Engineer	The learning path for a Physical Infrastructure Engineer entails designing and maintaining critical physical infrastructure, understanding building codes and standards, and assessing structural vulnerabilities.
Supply Chain Security Manager	A Supply Chain Security Manager's path includes securing supply chains, understanding supply chain risk management principles, assessing supplier security practices, and developing contingency plans.
Cyber Threat Intelligence Analyst	The learning path for a Cyber Threat Intelligence Analyst starts with courses in cyber threat intelligence collection and analysis, understanding threat actors and their methods, and proactive threat mitigation strategies.

2.2. Linking of Skills Profiles with Specific Skill Sets

The second step of our methodology was to break down the identified skills profiles into individual skills. The latter have been accordingly used to create clear and structured pathways for career advancement and skill development towards these skills. The analysis covered the needs of various stakeholder groups such as first responders, governments, analysts, and engineers. These insights indicated a clear path forward for stakeholders involved in CIP.

2.3. Construction of Learning Paths

The individual skills assigned to each profile led to construction of specific learning paths for each profile. To make each learning path more practical, we also mapped directly each path to one or more courses of the EU-CIP training catalogue, which is available within EU-CIP's knowledge hub[4]. At the time of writing of this version of the whitepaper, the EU-CIP training catalogue comprises over 140 CIP/CIR related courses, including courses developed by the EU-CIP project and courses produced by third-party providers. This made it generally possible to identify relevant courses that could match the skills of the various paths. However, it is also possible to accomplish the indicated learning paths based on other relevant courses i.e., courses outside the EU-CIP training catalogue. Overall, the presented learning paths can be seen as a guide for CI operators and security organizations to structure and deliver upskilling and reskilling activities for their employees. The delivery of these activities may or may not benefit from the EU-CIP courses and the EU-CIP training catalogue.

[4] https://knowledgehub.eucip.eu/training-courses/

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

3. Learning Paths Description

The tables in this section provide detailed learning paths for the above-listed fifteen CIP/CIR skills profiles. Each learning path description is structured in three sections:

- **Individual Skills of the Profile:** This section lists the essential skills required for professionals to effectively fulfil roles associated with each CIP/CIR skills profile. The skills listed are indicative and can be expanded based on emerging trends and the evolution of the professional roles that are linked to the profile.
- **Mandatory Courses of the Learning Path:** This part lists a curated list of courses that are essential for acquiring the skills specified in the profile. The courses are sourced from the EU-CIP Training Courses Catalogue and provide foundational pathway for skill acquisition. Given the dynamic nature of CIP/CIR, other similar courses from platforms like Udemy, Coursera and edX may also be suitable to support the acquisition of the key skills of the learning path.
- **Other Optional Courses:** In addition to the mandatory courses, this section suggests courses that could enhance the learning path. These courses are optional but recommended as they provide deeper insights or broader knowledge that complements the core mandatory skills.

Cybersecurity Specialist
Individual Skills of the Profile: • Proficiency in identifying and mitigating cyber threats. • Knowledge of encryption methods and security protocols. • Ability to conduct vulnerability assessments and penetration testing. • Familiarity with incident response procedures and forensic analysis.
Learning Path (Mandatory Courses): The Foundations of Cybersecurity, Coursera, University of Maryland, College Park Introduction to Cybersecurity & Risk Management Specialization, Coursera/UCI Critical Infrastructure Protection, TEEX - Texas A&M University Build Security Incident Response for GDPR data protection, Udemy Cybersecurity Compliance Framework & System Administration, Coursera/IBM Cybersecurity Risk and Strategy, edX/University of Connecticut Cybersecurity and Privacy in the IoT, edX/Curtin University
Learning Path (Optional Courses): Cybersecurity Threat Hunting for SOC Analyst, Udemy Understanding Indicators of Compromise, Cybersecurity and Infrastructure Security Agency (CISA) Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam AWS Certified Security Specialty 2023, Udemy

Table 1: Skills and Learning Path for the "Cybersecurity Specialist" Skills Profile

Risk Management Analyst
Individual Skills of the Profile: • Expertise in assessing risks to critical infrastructure. • Ability to develop risk management strategies and plans. • Proficiency in analysing data to identify potential vulnerabilities. • Strong communication skills to convey risk information effectively.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Learning Path (Mandatory Courses):
Introduction to Risk Management, edX/ColumbiX ISO 31000 - Enterprise Risk Management for the Professional, Udemy Risk Management Tools and Practices, edX/NYIF Cybersecurity Foundations for Risk Management, Coursera/Georgia University Detect and Mitigate Ethical Risks, Coursera/CertNexus Cybersecurity Compliance Framework & System Administration, Coursera/IBM Introduction to Business Continuity E-Learning Course, The Business Continuity Institute (BCI)
Learning Path (Optional Courses): Data: Law, Policy and Regulation, edX/ London School of Economics Dominant Risk Management Standards and Frameworks, Coursera/ University System of Georgia Data: Law, Policy and Regulation, edX/ London School of Economics Understanding Indicators of Compromise, Cybersecurity and Infrastructure Security Agency (CISA)

Table 2: Skills and Learning Path for the "Risk Management Analyst" Skills Profile

Emergency Response Coordinator
Individual Skills of the Profile: • Experience in coordinating response efforts during emergencies. • Knowledge of emergency management protocols and procedures. • Ability to communicate effectively with internal and external stakeholders during crisis situations. • Familiarity with incident command systems and emergency communication systems.
Learning Path (Mandatory Courses): Introduction to Cybersecurity & Risk Management Specialization, Coursera/UCI Security Analyst Fundamentals Specialization, Coursera/IBM ISO 27001:2022 Lead Implementer, Udemy IBM Cybersecurity Analyst Professional Certificate, Coursera/IBM Leadership in Emergency Management, Udemy Cybersecurity Compliance Framework & System Administration, Coursera/IBM MGT551: Building and Leading Security Operations Centers, SANS Institute Crisis Communications, Coursera/IESE Business School
Learning Path (Optional Courses): Critical Infrastructure Protection, TEEX - Texas A&M University Misinformation and Disinformation Training, Management and Strategy Institute Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam Build Security Incident Response for GDPR data protection, Udemy

Table 3: Skills and Learning Path for the "Emergency Response Coordinator" Skills Profile

Physical Security Specialist
Individual Skills of the Profile: ▪ Proficiency in designing and implementing physical security measures. ▪ Knowledge of access control systems and surveillance technologies. ▪ Experience in conducting security assessments and audits.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

▪ Ability to develop security policies and procedures.
Learning Path (Mandatory Courses): Intro to the Physical Security Industry, Udemy The Foundations of Cybersecurity, Coursera, University of Maryland, College Park Physical and Advanced Side-Channel Attacks, edX/ TUGrazX The Complete Cyber Security Course : Hackers Exposed!, Udemy Dominant Risk Management Standards and Frameworks, Coursera/ University System of Georgia CCTV Cameras From Scratch : Security Camera System, Udemy MGT551: Building and Leading Security Operations Centers, SANS institute
Learning Path (Optional Courses): Build Security Incident Response for GDPR data protection, Udemy Applied Control Systems 3: UAV drone (3D Dynamics & control), Udemy SEC511: Continuous Monitoring and Security Operations, SANS Institute Endpoints and Systems, Coursera/Cisco

Table 4: Skills and Learning Path for the "Physical Security Specialist" Skills Profile

Network Infrastructure Engineer
Individual Skills of the Profile: ▪ Expertise in designing and maintaining network infrastructure. ▪ Knowledge of network protocols and technologies. ▪ Ability to troubleshoot network issues and optimize performance. ▪ Familiarity with network security principles and best practices.
Learning Path (Mandatory Courses): The Foundations of Cybersecurity, Coursera, University of Maryland, College Park Networking Fundamentals, Coursera/Akamai Introduction to Network Protocols, Coursera/University System of Georgia VPC Networking: Cloud HA-VPN, Coursera/Google Cloud Real-Time Cyber Threat Detection and Mitigation, Coursera/NYU Introduction to Software Defined Networking, edx/CurtinX Google Cybersecurity Professional Certificate, Coursera/Google
Learning Path (Optional Courses): SEC511: Continuous Monitoring and Security Operations, SANS Institute Build Security Incident Response for GDPR data protection, Udemy Applied Control Systems 3: UAV drone (3D Dynamics & control), Udemy Endpoints and Systems, Coursera/Cisco

Table 5: Skills and Learning Path for the "Network Infrastructure Engineer" Skills Profile

Critical Infrastructure Resilience Planner
Individual Skills of the Profile: ▪ Experience in developing resilience plans for critical infrastructure. ▪ Knowledge of resilience frameworks and methodologies. ▪ Ability to conduct risk assessments and prioritize mitigation efforts. ▪ Strong analytical and problem-solving skills.
Learning Path (Mandatory Courses):

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

System Administration and IT Infrastructure Services, Coursera/Google Protecting Critical National Infrastructure, Cranfield University Introduction to Cybersecurity & Risk Management Specialization, Coursera/UCI Cybersecurity Risk and Strategy, edX/University of Connecticut Cybersecurity Capstone: Breach Response Case Studies, Coursera/IBM Crisis Communications, Coursera/IESE Business School Cybersecurity Compliance Framework & System Administration, Coursera/IBM
Learning Path (Optional Courses): Build Security Incident Response for GDPR data protection, Udemy Introduction to Business Continuity E-Learning Course, The Business Continuity Institute (BCI) Organizational Crisis Leadership E-Learning Course, The Business Continuity Institute (BCI) Dominant Risk Management Standards and Frameworks, Coursera/ University System of Georgia

Table 6: Skills and Learning Path for the "Critical Infrastructure Planner" Skills Profile

Incident Response Manager
Individual Skills of the Profile: ▪ Proficiency in managing incident response teams. ▪ Experience in developing and implementing incident response plans. ▪ Knowledge of forensic analysis techniques and evidence preservation. ▪ Ability to coordinate with law enforcement and regulatory agencies during investigations.
Learning Path (Mandatory Courses): Introduction to Cybersecurity & Risk Management Specialization, Coursera/UCI IBM Cybersecurity Analyst Professional Certificate, Coursera/IBM Leadership in Emergency Management, Udemy Cybersecurity Compliance Framework & System Administration, Coursera/IBM MGT551: Building and Leading Security Operations Centers, SANS Institute Crisis Communications, Coursera/IESE Business School Cybersecurity Capstone: Breach Response Case Studies, Coursera/IBM
Learning Path (Optional Courses): Critical Infrastructure Protection, TEEX - Texas A&M University Misinformation and Disinformation Training, Management and Strategy Institute Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam Build Security Incident Response for GDPR data protection, Udemy

Table 7: Skills and Learning Path for the "Incident Response Manager" Skills Profile

Compliance Auditor
Individual Skills of the Profile: ▪ Expertise in auditing critical infrastructure for compliance with regulations and standards. ▪ Knowledge of relevant regulatory frameworks and industry guidelines. ▪ Ability to conduct compliance assessments and identify gaps. ▪ Strong attention to detail and analytical skills.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Learning Path (Mandatory Courses):
Cybersecurity Compliance Framework & System Administration, Coursera/IBM IBM: Cybersecurity Compliance and System Administration, edX/IBM Enterprise and Infrastructure Security, Coursera/NYU Data Analysis and Visualization Foundations Specialization, Coursera/IBM Modern Internal Audit Leadership, Udemy Fundamentals of Compliance Auditing, The Institute of Internal Auditors Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam
Learning Path (Optional Courses):
Data Ethics, AI and Responsible Innovation, edX/ University of Edinburgh Data: Law, Policy and Regulation, edX/ London School of Economics Crisis Communications, Coursera/IESE Business School CertNexus Certified Ethical Emerging Technologist Professional Certificate, Coursera/CertNexus

Table 8: Skills and Learning Path for the "Compliance Auditor" Skills Profile

Industrial Control Systems (ICS) Engineer
Individual Skills of the Profile: ▪ Experience in designing and maintaining industrial control systems. ▪ Knowledge of SCADA (Supervisory Control and Data Acquisition) systems and protocols. ▪ Ability to assess and mitigate cyber threats targeting ICS. ▪ Familiarity with industry-specific regulations and best practices.
Learning Path (Mandatory Courses):
Applied Control Systems 3: UAV drone (3D Dynamics & control), Udemy AlaskaX: Unmanned Aerial Systems (UAS): Fundamentals, edX/AlaskaX Learn SCADA from Scratch - Design, Program and Interface, Udemy PLC Fundamentals (Level I), Udemy HMI Interfacing with PLC, Udemy Cybersecurity Compliance Framework & System Administration, Coursera/IBM Advanced Process Control & Safety Instrumented Systems SIS, Udemy
Learning Path (Optional Courses):
Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam Data: Law, Policy and Regulation, edX/ London School of Economics Crisis Communications, Coursera/IESE Business School Networking Fundamentals, edX/CurtinX

Table 9: Skills and Learning Path for the "Industrial Control Systems (ICS) Engineer" Skills Profile

Crisis Communication Specialist
Individual Skills of the Profile: ▪ Communicating Messages about Crisis ▪ Clear and Concise Messaging about Security Issues ▪ Rapid Response and Adaptability ▪ Customizing Communication for Diverse Audiences

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

▪ Emotional Intelligence and Empathy ▪ Trusted Communications
Learning Path (Mandatory Courses): Crisis Communications, Coursera/IESE Business School Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam Organizational Crisis Leadership E-Learning Course, The Business Continuity Institute (BCI) Build Security Incident Response for GDPR data protection, Udemy Reputation Management in a Digital World, edX/Curtin Crisis Communication Management Certification Course, Institute for Crisis Management Fighting Misinformation: Digital Media Literacy, International Research & Exchanges Board
Learning Path (Optional Courses): Data Ethics, AI and Responsible Innovation, edX/ University of Edinburgh Misinformation and Disinformation Training, Management and Strategy Institute Data: Law, Policy and Regulation, edX/ London School of Economics Fake News, Facts, and Alternative Facts, edX/University of Michigan

Table 10: Skills and Learning Path for the "Crisis Communication Specialist" Skills Profile

Business Continuity Planner
Individual Skills of the Profile: ▪ Expertise in developing business continuity plans for critical infrastructure. ▪ Knowledge of continuity planning frameworks and methodologies. ▪ Ability to identify and prioritize critical business functions. ▪ Experience in conducting continuity exercises and simulations.
Learning Path (Mandatory Courses): Introduction to Business Continuity E-Learning Course, The Business Continuity Institute (BCI) Organizational Crisis Leadership E-Learning Course, The Business Continuity Institute (BCI) Cybersecurity: Developing a Program for Your Business Specialization, Coursera/Georgia University Dominant Risk Management Standards and Frameworks, Coursera/ University System of Georgia Cybersecurity Foundations for Risk Management, Coursera/Georgia University Cybersecurity Compliance Framework & System Administration, Coursera/IBM Data: Law, Policy and Regulation, edX/ London School of Economics Crisis Communications, Coursera/IESE Business School
Learning Path (Optional Courses): Data Ethics, AI and Responsible Innovation, edX/ University of Edinburgh Data Analysis and Visualization Foundations Specialization, Coursera/IBM Science Communication: Communicating Trustworthy Information in the Digital World, Coursera/Erasmus University Rotterdam Business Continuity Basics, The Business Continuity Institute (BCI)

Table 11: Skills and Learning Path for the "Business Continuity Planner" Skills Profile

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Data Protection Officer (DPO)
Individual Skills of the Profile: Proficiency in ensuring compliance with data privacy regulations. Knowledge of data protection laws and standards. Ability to assess data privacy risks and develop mitigation strategies. Experience in managing data breach incidents and conducting investigations.
Learning Path (Mandatory Courses): Cybersecurity Compliance Framework & System Administration, Coursera/IBM Build Security Incident Response for GDPR data protection, Udemy Cybersecurity Capstone: Breach Response Case Studies, Coursera/IBM Data Ethics, AI and Responsible Innovation, edX/ University of Edinburgh IBM: Cybersecurity Compliance and System Administration, edX/IBM Data: Law, Policy and Regulation, edX/ London School of Economics How to succeed in a Data Protection Officer Role (GDPR DPO), Udemy
Learning Path (Optional Courses): Gen AI for Data Privacy & Protection, Coursera/Edureka Dell Technologies Data Protection Design, Udemy IBM Cybersecurity Analyst Professional Certificate, Coursera/IBM AI and Disaster Management, Coursera/ DeepLearning.ai

Table 12: Skills and Learning Path for the "Data Protection Officer (DPO)" Skills Profile

Physical Infrastructure Engineer
Individual Skills of the Profile: ▪ Experience in designing and maintaining physical infrastructure for critical facilities. ▪ Knowledge of building codes and construction standards. ▪ Ability to assess structural vulnerabilities and recommend improvements. ▪ Familiarity with disaster-resistant building techniques and technologies.
Learning Path (Mandatory Courses): Introduction to Engineering and Design, edX/ BrownX Transportation, Sustainable Buildings, Green Construction, Coursera/John Hopkins Management of Urban Infrastructures, Coursera/EPFL Intro to the Physical Security Industry, Udemy Energy Within Environmental Constraints, edX/HarvardX EPFLx: A Resilient Future: Science and Technology for Disaster Risk Reduction, edX/EPFL Understanding Indicators of Compromise, Cybersecurity and Infrastructure Security Agency (CISA)
Learning Path (Optional Courses): Sustainable Construction Management, edX/University of Maryland Build Security Incident Response for GDPR data protection, Udemy Dominant Risk Management Standards and Frameworks, Coursera/ University System of Georgia Physical and Advanced Side-Channel Attacks, edX/ TUGrazX

Table 13: Skills and Learning Path for the "Physical Infrastructure Engineer" Skills Profile

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

Supply Chain Security Manager
Individual Skills of the Profile: ▪ Expertise in securing supply chains for critical infrastructure. ▪ Knowledge of supply chain risk management principles. ▪ Ability to assess supplier security practices and enforce compliance. ▪ Experience in developing contingency plans for supply chain disruptions.
Learning Path (Mandatory Courses): Supply Chain Fundamentals, edX/MIT Cybersecurity Compliance Framework & System Administration, Coursera/IBM Cybersecurity Foundations for Risk Management, Coursera/Georgia University Supply Chain Risk Management(SCRM) ISO/IEC27036 / ISO28000, Udemy Gen AI for Data Privacy & Protection, Coursera/Edureka IT Security: Defense against the digital dark arts, Coursera/Google Introduction to Business Continuity E-Learning Course, The Business Continuity Institute (BCI)
Learning Path (Optional Courses): Introduction to Physical Security in Critical Infrastructure Protection, EU-CIP Strategies for Supply Chain Digitalization, edX/ IMD Data Ethics, AI and Responsible Innovation, edX/ University of Edinburgh Business Continuity Basics, The Business Continuity Institute (BCI)

Table 14:Skills and Learning Path for the "Supply Chain Security Manager" Skills Profile

Cyber Threat Intelligence Analyst
Individual Skills of the Profile: ▪ Proficiency in collecting and analysing cyber threat intelligence. ▪ Knowledge of threat actors and their tactics, techniques, and procedures (TTPs). ▪ Ability to produce actionable intelligence reports for decision-makers. ▪ Experience in threat hunting and proactive threat mitigation strategies.
Learning Path (Mandatory Courses): The Foundations of Cybersecurity, Coursera, University of Maryland, College Park Endpoints and Systems, Coursera/Cisco The Complete Cyber Security Course : Hackers Exposed!, Udemy MGT551: Building and Leading Security Operations Centers, SANS institute Cyber Threat Intelligence, Udemy IBM Cybersecurity Analyst Professional Certificate, Coursera/IBM Google Cybersecurity Professional Certificate, Coursera/Google Cybersecurity Capture the Flag (CTF) Competition Training, TONEX
Learning Path (Optional Courses): Digital Forensics Concepts, Coursera/Infosec Data Analysis and Visualization Foundations Specialization, Coursera/IBM Cybersecurity Threat Hunting for SOC Analyst, Udemy Understanding Indicators of Compromise, Cybersecurity and Infrastructure Security Agency (CISA)

Table 15: Skills and Learning Path for the "Cyber threat Intellifence Analyst" Skills Profile

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

4. Outlook: How to Use the Whitepaper and How to Engage

Security organizations, training organizations, CI operators and other CIP/CIR stakeholders can use the above-listed learning paths to plan training, upskilling and reskilling activities. Moreover, human resources departments can consider the presented learning paths in the specification of career development roadmaps. Apart from fostering the development of special skillsets for critical infrastructure protection, most of the listed learning paths also serve the following objectives:

- They empower CIP professionals to learning to use and facilitate new tools and technologies.
- They boost resilient learning such as learning by following unexceptional event flows, anomalies and early warning signs, which is important in roles that have to proactively and intelligently cope with security incidents.

Most of the courses that are associated with the presented learning paths are available through the EU-CIP knowledge hub, which provides a single point of access to the educational resources referenced within this whitepaper. This can substantially help training development stakeholders to locate relevant courses for the presented learning paths.

Furthermore, EU-CIP encourages stakeholders to engage with the proposed learning paths in order to contribute to their evolution, while proposing other important learning paths that are missing from the initial list. To this end, a dedicated section on the EU-CIP Knowledge Hub can be leveraged to provide feedback and suggestions. The section comprises a feedback form, which enables stakeholders to propose new skills profiles or suggest modifications to existing ones.

Note that this is the first version and release of the EU-CIP skills and learning paths whitepapers. Considering feedback and suggestions received from different CIP training actors, EU-CIP will provide relevant revisions and enhancements to the present whitepaper.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.

References

[EC23a] European Commission. (2023) Mind the Cyber Skills Gap: a deep dive into Cybersecurity. Digital Skills & Jobs Platform. Available at: https://digital-skills-jobs.europa.eu/en/latest/briefs/mind-cyber-skills-gap-deep-dive (Accessed: 16 May 2024).

[EC23b] European Commission. (2023) Cybersecurity Skills Academy. Digital Skills & Jobs Platform. Available at: https://digital-skills-jobs.europa.eu/en/cybersecurity-skills-academy (Accessed: 16 May 2024).

World Economic Forum (2024) 'The 2020s will be a decade of upskilling: Employers should take notice', World Economic Forum, 5 January. Available at: https://www.weforum.org/agenda/2024/01/the-2020s-will-be-a-decade-of-upskilling-employers-should-take-notice/ (Accessed: 12 May 2024).

ISACA (2023) 'New ISACA research: 59 percent of cybersecurity teams are understaffed', ISACA, 25 April. Available at: https://www.isaca.org/about-us/newsroom/press-releases/2023/new-isaca-research-59-percent-of-cybersecurity-teams-are-understaffed (Accessed: 12 May 2024).

Scale Venture Partners (2023) Scale Security Report 2023. Available at: https://www.scalevp.com/wp-content/uploads/2023/10/Scale-Security-Report-2023-Final.pdf (Accessed: 12 May 2024).

List of Skills and Learning Paths

Consortium:

Engineering – Ingegneria Informatica SPA (ENG), Italy
Deutsches Zentrum für Luft und Raumfahrt EV (DLR), Germany
GFT Italia SRL (GFT), Italy
Inov instituto de engenharia de sistemas e computadores inovacao (INOV), Portugal
Inlecom commercial pathways company limited by guarantee (ICP), Ireland
SINTEF AS (SIN), Norway
Steinbeis EU-VRI GMBH (EU-VRi), Germany
Stowarzyszenie Polska Platforma bezpieczenstwa wewnetrznego (PPHS), Poland
Laurea – Ammattikorkeakoulou oy (LAU), Finland
Innov - Acts Limited (INNOV), Cyprus
Norks Regnesentral (NRS), Norway
European Organisation for Security (EOS), Belgium
Katholieke Universiteit Leuven (KUL), Belgium
Fstechnology SPA (FST), Italy
Athens International Airport S.A (AIA), Greece

This project has received funding from the European Union’s Horizon Europe research and innovation programme under the grant agreement No 101073878.

Fundacion de la Comunidad Valenciana para la investigacion, promocion y estudios comerciales de Valenciaport (FV), Spain
Orange Romania (ORO), Romania

Electricité de France (EDF), France
Association française de normalisation (AFNOR), France
Leonardo Societa per Azioni (LDO), Italy

Contact:

Project Coordinator: Emilia Gugliandolo (ENG)

Whitepaper Contact: John Soldatos (INNOV)

Dissemination Manager: Elodie Reuge (EOS)

Funded by the European Union

*Disclaimer: Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Commission. Neither the European Union nor the granting authority can be held responsible for them.

This project has received funding from the European Union's Horizon Europe research and innovation programme under the grant agreement No 101073878.