Charter of Trust

Cybersecurity Policy Manifesto

Publication date: 12 April 2024

Charter of Trust –
Classification CoT Public

Executive Summary

The Charter of Trust presents this Manifesto as a call to action for Policymakers to join forces in the pursuit of a secure and resilient digital environment. As a collective of leading technology, cybersecurity, and industry stakeholders, we believe that a united and collaborative approach is essential for effectively combating cyber threats that endanger the security, privacy, and prosperity of our societies.

Our vision is to establish a strong, secure, and resilient digital Europe that fosters innovation, economic growth, and social progress while protecting individual rights and safeguarding the values of a democratic society.

Introduction

In today's rapidly evolving geopolitical landscape marked by conflicts, economic challenges, an ever-growing threat landscape, addressing cybersecurity issues has become increasingly critical.

In parallel, companies also have to navigate a complex and interconnected mosaic of legislations that have been adopted across regions. More specifically, both the EU and US have been actively working on strengthening their legislative frameworks to enhance their global cyber resilience, safeguarding communications and data in multiple sectors that have become increasingly dependent on digital technologies (energy, economy, healthcare, financial sectors, etc.), somewhat adding a level of uncertainty as to the obligations and compliance requirements put on businesses that operate in this these fields.

As such, overlapping legislative systems across these sectors could prove ineffective for the growing concerns of modern cybersecurity in the future. This, along with the recent crisis such as COVID-19 global pandemic and the ongoing Russia's war of aggression against Ukraine, has prompted the need for an even more comprehensive cybersecurity regulative framework.

Charter of Trust recommendations

Protecting our supply chains and infrastructures and ensuring their resilience by:

- **Leveraging on existing international standards to further facilitate convergent standard development, fair equivalences and compliance**. We believe that a connected world needs certification schemes that meet the unique challenges of IoT device security, while reducing cost and complexity for developers. As prominent industry leaders, the Charter of Trust Partners remain determined to engage with regulators to effectively contribute to the development of EU's cybersecurity standards, certification schemes, conformity assessment criteria, based on existing international best practices. We also welcome ENISA's mapping of existing standards in the context of the Cyber Resilience Act (CRA) implementation. Going forward, it is key to include industry in the relevant consultations on CRA standardisation to leverage industry best practices and technology expertise.
- **Developing a consistent and harmonized policy framework** across the European Union that facilitates cross-border collaboration and information sharing. As we are now entering into an important regulatory implementation phase following the adoption of several essential legislations such as the NIS 2 Directive, DORA, the CRA, and the Cyber Solidarity Act (CSA), there is a need to ensure effective alignment among national cybersecurity strategies, regulatory and reporting requirements across sectors and countries. . In particular, it is essential to streamline the reporting requirements stemming from these different legislative frameworks and develop single entry points for reporting on the national level. Similarly, the Charter of Trust Partners call for further harmonisation at a global level of baseline requirements for products, functionalities, technologies, processes, operations and architectures. This can be achieved through further implementation of initiatives like the EU-US CyberSafe Product Action

Plan which strives to enhance technological collaboration in order to achieve mutual recognition concerning cybersecurity prerequisites for Internet-of-things (IoT) hardware and software consumer goods.

- **Implementing rigorous supply chain risk assessments** to prevent vulnerabilities in hardware, software, and services. We welcome the US Software Bill of Materials (SBOM) which has become an increasingly important tool for providing much-needed clarity about the components that make up a software — both for application security purposes and governmental compliance. The Charter of Trust recommends further alignment of the SBOM standards and templates with an international approach to enhance resilience of our supply chains in a globally harmonized manner. Charter of Trust Partners encourage as well implementation of secure development lifecycle and exchange of best practices among industry and throughout the supply chain.

Advance on research and make policy future-proof amid emerging technologies:

- **Quantum-Safe Cryptography**: The Charter of Trust encourages further collaboration on quantum-resistant encryption methods to protect against future quantum computing threats. The ability of quantum computers to instantly perform massive calculations threatens the currently used encryption systems across every digital connection imaginable. Recent technological advancements in this domain highlight the urgency of implementing quantum secure solutions. Delaying the migration to post-quantum cryptography risks leaving systems vulnerable to exploitation by entities with access to quantum computing capabilities. This threat is further exacerbated by the possibility of harvesting stolen data and deciphering it at a later date. There is, therefore, an increasing time pressure for critical infrastructure to start planning the migration of their networks to post-quantum cryptography. The Charter of Trust Partners call on the European Institutions to adjust their existing policy approaches (e.g. implementation of the NIS2 Directive) to the emerging cybersecurity challenges by leveraging on existing standards and collaborate with trusted industry partners on government programmes and promote the migration of the critical assets to quantum-safe solutions.
- **AI and Machine Learning**: The Charter of Trust supports leveraging artificial intelligence and machine learning for proactive threat detection and adaptive cyber protection. Businesses of all sizes operating in EU Single Market require legal clarity and direction on the implementation of the provisions of the AI Act. Regulatory intricacy should not hinder European technological competitiveness, innovation, or discourage investment. It is crucial to minimize the risk of different interpretations or implementation ways of the EU AI Act in the Single Market, especially as Member States consider appointing diverse lead authorities for enforcing the Act. Collaboration at the global level regarding fundamental AI governance principles remains imperative. Together with supporting the implementation of the AI Act, the next EU mandate should continue to investigate how the EU can enhance AI adoption, as well as foster the creation and implementation of innovative AI applications.

Training, education and raising awareness

- **The Charter of Trust Partners advocate for increased investments in cybersecurity education and awareness** campaigns to empower individuals, businesses, and public institutions with the knowledge and skills necessary to protect themselves against cyber threats. This includes supporting training programs, research initiatives, and public awareness campaigns. We welcome the European Commission initiative to set up a Cyber Skills Academy and are open to partner with government stakeholders on its active implementation.
- **The Charter of Trust Partners endorse the strengthening of dialogue and partnership** with both industry and academia to better understand the evolving skills demand and trends on the job market impacted by the rapid adoption of new technologies (i.e. AI). Partnerships with private stakeholders and academia allow to develop targeted skilling programs for professionals based on current job market demand.

Strengthening Cooperation

- **Align standards and policy approaches with international partners is key to our common cyber resilience**. Joint initiatives and collaboration is one of the founding principles of the Charter of Trust alliance. Our Partners remain active in fostering collaboration between EU-US industry stakeholders, national agencies and policymakers as it is crucial to ensure and promote alignment of standards and policy approaches. Working with industry would allow for a better assessment of market needs and make informed policy decisions.
- **We recommend improving information sharing by leveraging on the frameworks developed as part of the EU Cyber Solidarity Act** such as the European Cybersecurity Alert System, the Cybersecurity Emergency Mechanisms and the European Cybersecurity Incident Review Mechanisms These platforms can foster information sharing not only within the EU but also with trusted external partners. The Charter of Trust Partners remain engaged in facilitating trusted information exchange mechanisms at all levels and among relevant parties.

Charter of Trust

The Charter of Trust

Protecting the digital world of tomorrow

About the Charter of Trust

The Charter of Trust is a non-profit alliance of leading global companies and organisations working across sectors to make the digital world of tomorrow a safer place. It was founded in 2018 at the Munich Security Conference to enhance cybersecurity efforts and foster digital trust in the face of an increasingly complex and severe cyber threat landscape.

A unique initiative underpinned by 10 principles fundamental to a secure digital world, the Charter of Trust is working to protect our increasingly digitized world and build a reliable foundation on which trust and digital innovation can flourish. It contributes to the development of effective cybersecurity policies that strengthen global cybersecurity posture and provides expertise on topics including AI, security by default, supply chain security, and education

Objectives

The Charter of Trust seeks to harmonize cybersecurity approaches and address cybersecurity challenges from a holistic, ethical and fair perspective. The alliance is collaborating across industries to cultivate, advocate, and enhance global cybersecurity standards. By fostering widespread awareness and sharing expertise, it ensures a cohesive approach to security that enables seamless global interoperability.

Key principles

The work of the Charter of Trust is underpinned by 10 principles fundamental to a secure digital world:

1. Ownership for cyber and IT security
2. Responsibility throughout the digital supply chain
3. Security by default
4. User-centricity
5. Innovation and co-creation
6. Education
7. Cyber-resilience through conformity and certification
8. Transparency and response
9. Regulatory framework
10. Joint initiatives

Contact

contact@charteroftrust.info