Transatlantic Business Initiative

Enhanced public-private transatlantic cooperation to foster transatlantic cyber-resilience

Six policy Recommendations on Cybersecurity for the Fifth Ministerial Meeting of the transatlantic Trade and Technology Council

September 2023

The global cyber threat necessitates transatlantic cooperation

The global cyber threat landscape is continuously growing. If cybercrime was a country, it would rank as the third largest economy behind the US and China as cyber-crime-inflicted damages are estimated at 8 trillion USD in 2023.[1] In the United States of America, the damage caused by cyber-incidents and cyber-enabled frauds reported to the Federal Bureau of Investigation (FBI) amounted to 10.2 billion USD in 2022 alone – an increase by almost 48 per cent in comparison to 2021.[2] While comparable figures are not available for the EU, the continuously high level of reported cyber-attacks leads to the assumption that the rates would be similarly high. Since the number of connected devices is expected to almost double between 2023 and 2030 leading to almost 30 billion devices, it is fair to assume that the damage caused by cyber-incidents will continue to rise.[3] Attackers only have to find one vulnerability they can exploit while operators of IT systems have to protect their entire infrastructure. Since cybercriminals are operating at a global scale and cyberattacks can be purchased as a service, cooperation and collaboration among partners is paramount to enhance the cyber-resilience of countries, companies and citizens alike.

Therefore, German businesses urge policymakers on both sides of the Atlantic to:

(1) Involve businesses in the framework of the US-EU-Cyber-Dialogue,
(2) Harmonize regulatory requirements,
(3) Work towards mutual recognition of product-related cybersecurity certifications,
(4) Align reporting obligations,
(5) Connect existing cyber-threat information-sharing mechanisms to enhance knowledge diffusion between businesses and public bodies, and
(6) Step up joint efforts to bridge the skill and expert gaps.

[1] CybercrimeMagazine. 2020. Cybercrime To Cost The World 8 Trillion Annually In 2023. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/
[2] FBI. 2022. Internet Crime Report 2022. https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf
[3] Statista. 2022. Number of Internet of Things (IoT) connected devices worldwide from 2019 to 2021, with forecasts from 2022 to 2030. https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

German businesses' policy recommendations

Given the escalating threat landscape – with cyberattacks increasing both in quantity and sophistication – German businesses urge the US Administration and the European Commission to utilize the transatlantic Trade and Technology Council to deepen their cooperation in the area of cybersecurity. To this end, we would appreciate, if the negotiations were to agree on the following measures during the fifth ministerial meeting of the Trade and Technology Council:

Involve businesses in the framework of the US-EU-Cyber-Dialogue

The Transatlantic Business Initiative (TBI) welcomes official exchanges from the US Administration and the EU institutions exchange within the framework of the US-EU-Cyber-Dialogue on a regular basis about a range of topics, including updates on respective cyber policy frameworks, cooperation in multilateral fora, cyber diplomacy and deterrence, collaboration on crisis response, resilience as well as capacity building in third countries. German business would appreciate, if apart from government officials, business representatives were also allowed to join this format. Companies could provide direct input on their cyber-resilience strategies and share knowledge directly with European and US government counterparts.

Harmonize regulatory requirements

German businesses active on both sides of the Atlantic are increasingly confronted with a plethora of different and often diverging regulatory approaches to cyberspace – such as differing reporting mechanisms, definitions, and requirements in public procurement processes. This rising regulatory complexity results in additional compliance costs for companies without enhancing the cyber-resilience of companies, public entities, or society writ large. Rather, it forces companies to invest scarce IT security personnel to adapt their internal security processes according to local, national or supranational requirements, rather than hardening their systems and products. Therefore, German businesses urge the EU Member States to implement the requirements emanating from the NIS 2 Directive in a uniform manner and for the US to harmonize the cybersecurity requirements established across the US States. Henceforth, German businesses welcome that the National Cybersecurity Strategy Implementation Plan initiative number 1.1.1 encourages the Office of the National Cyber Director to liaise with independent and executive branch regulators to harmonize baseline cybersecurity requirements. German businesses – both operators of critical infrastructure as well as other companies – would appreciate being involved in the upcoming stakeholder consultation.

Ideally, the EU and the US should work within the framework of the Transatlantic Trade and Technology Council towards the complete harmonization of cybersecurity requirements and policies. In additional, both partners should agree on a set of internationally recognized standards –

developed within international standardization bodies – that underpin the respective regulatory framework.

Work towards mutual recognition of product-related cybersecurity certifications

Currently, the EU is working towards the introduction of horizontal cybersecurity requirements for all products with digital elements within the framework of the Cyber Resilience Act. Producers of products with digital elements will have to assess the conformity of their products against European or international technical standards or will even have to obtain a certification by a third party. At the same time, the US National Cybersecurity Strategy Implementation Plan foresees in initiative number 1.2.1 the development of security-by-design and security-by-default principles and practices by CISA and NIST together with other relevant stakeholders. German industry offers to contribute to the development of such principles and practices as we regard risk-adequate cybersecurity requirements for all products and services paramount to the increase of global cyber-resilience.

The European Commission and the US Administration should update existing Mutual Recognition Agreements (MRA) for Conformity Assessment to apply them to the Cyber Resilience Act. The principle of reciprocity eliminates duplication by accepting the entities' assessments or certification in lieu of one's own. Such mutual recognitions are paramount to reduce the bureaucratic burden associated with multiple certifications/self-assessments. Moreover, it will help companies to focus their scarce cybersecurity capacities on developing cyber-resilient products or maintaining the cyber-resilience of their systems respectively. In addition, MRA for conformity assessments will also help reduce potential bottlenecks in conformity assessment bodies since each product would only have to be tested either in the US or Europe.

Align reporting obligations

Both the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) in the US as well as the Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive) oblige operators of critical infrastructures – and in case of the NIS 2 Directive also many other companies – to report cybersecurity incidents. Currently, the legal frameworks in the US and in the EU differs in terms of which incidents must be reported, who has to report them, and timeframes for entities have to report cybersecurity incidents and / or vulnerabilities. German businesses would appreciate if the US Administration and the European Commission were to agree on harmonizing their cybersecurity incident requirements as well as the subsequent reporting mechanisms.

For example, German businesses recommend that the NIS 2's reporting mirrors the one under the CIRCIA. The CIRCIA requires covered entities that experience a covered cyber incident to

report the covered cyber incident to the Agency not later than 72 hours after the covered entity reasonably believes that the covered cyber-incident has occurred. In contrast, under NIS 2 an initial information must be provided to the national cybersecurity authority within 24 hours. Likewise, German businesses would welcome an agreement between the US and the EU Member States on a common reporting mechanism. This would facilitate the reporting process especially for globally operating enterprises.

Connect existing cyber-threat information-sharing mechanisms to enhance knowledge diffusion between businesses and public bodies

A speedy exchange of information about new attack and threat vectors is paramount for an effective and timely response to new cyber threats. At the same time, various platforms to exchange information about cyber-incidents as well as vulnerabilities exist on both sides of the Atlantic. The knowledge exchanged on these platforms, however, is not exchanged between these platforms. Thereby, information silos exist, which hamper the speedy strengthening of companies' and states' cyber-resilience. This provides malicious cyber actors with a significant advantage.

Therefore, German businesses urge the European Commission and the US-Administration to establish digital interfaces between existing information sharing platforms by 2024 to enhance a speedy information exchange between national cybersecurity agencies and businesses. National cybersecurity agencies should be encouraged to publish information about new threat vectors, while businesses should strive to inform private as well as public third parties about cyberthreats they become aware of when monitoring their own systems. Equally important would be an information mechanism about the disclosure of vulnerabilities and respective remedies as well as a banning the use of back doors and zero-day exploits by public bodies. Business representatives should be included in the process of setting up the necessary technical interfaces between existing information sharing tool to ensure that they mirror their requirements in terms of trustworthiness and data protection. Improving the information basis will help companies to swiftly adapt their security strategies in case of new zero-day exploits as well as other newly emerging threat vectors.

Step up joint efforts to bridge the skill and expert gaps

According to recent studies, the cybersecurity expert gap amounts to 410,000 in the US and 317,000 in the EMEA region. At a global scale, the cybersecurity workforce gap is currently

growing twice as much as the cybersecurity workforce.[4] German businesses accordingly urge European and US-American policymakers to step up efforts to close the skills and experts gaps.

Consequently, German businesses welcome the Biden-Harris Administration's recent announcement of a National Cyber Workforce and Education Strategy. We agree with the Administration's assessment that "filling the hundreds of thousands of cyber job vacancies across our nation is a national security imperative" – this analysis holds likewise true for the European Union. We applaud the strategy's four pillars, as they will help – if thoroughly implemented – to enhance the overall cyber-resilience of the US. Especially pillar one, which seeks to "equip every American with foundational cyber-skills", in conjunction with pillar two, which aims at "transforming cyber education", are vital steps to augment overall cyber-awareness by providing every citizen with necessary cybersecurity information based on state-of-the-art teaching approaches. From a business perspective, the strategy's third pillar is of outmost importance as it seeks to bridge the above stated expert gap.

German businesses welcome efforts between European and US policymakers were to exchange best practices, set up new dedicated cybersecurity courses at higher education institutions, and implement cybersecurity awareness trainings as part of life-long learning strategies. We encourage the US. Administration to partner with its European allies when implementing its National Cyber Workforce and Education Strategy.

Currently, only 25 per cent of IT security jobs are filled by women globally.[5] While this is a considerable increase in comparison to 2013, when only ten per cent of all IT security posts were filled by women, governments should support initiatives promoting an increasing uptake of IT jobs by women, such as #SheTransformsIT, as well as enhance the attractiveness of STEM courses at all educational levels. Closing the cybersecurity gender gap is crucial to close the overall cybersecurity workforce gap.

[4] (ISC)². 2022. Cybersecurity Workforce Study. https://www.isc2.org/Research/Workforce-Study#
[5] eSENTIRE / Cybersecurity Ventures. 2022. Cybercrime Report. https://s3.ca-central-1.amazonaws.com/esentire-dot-com-assets/assets/resourcefiles/2022-Official-Cybercrime-Report.pdf

About the TBI

The Transatlantic Business Initiative (TBI) is the point of contact for economic policy issues, particularly for the German government and the governments of the United States and Canada as well as for EU institutions. The initiative is supported by four business associations: the Federation of German Industries (BDI), the Association of German Chambers of Industry and Commerce (DIHK), the Federation of German Wholesale, Foreign Trade and Services (BGA) and the Association of German Banks (BdB) and advocates for strengthening the economic relations between Germany and the European Union on the one hand, and the United States and Canada on the other. Members of the TBI work in four steering committees, focusing in particular on trade and investment policy, energy and climate policy, data and the digital economy as well as business and finance, and seek to engage with policymakers, regulators and supervisors, business and trade representatives as well as other stakeholders to strengthen transatlantic ties and facilitate coordination on matters of shared interest.

Imprint

Transatlantic Business Initiative (TBI)
www.transatlanticbusiness.eu
c/o Bundesverband der Deutschen Industrie e.V. (BDI)
Breite Straße 29, 10178 Berlin
Phone: +49 30 2028-0
www.transatlanticbusiness.eu

Editors

Steven Heckler
Deputy Head of Department Digitalization and Innovation
Federation of German Industries
Phone: +49 30 2028-1523
E-mail: s.heckler@bdi.eu

With research support by Sven Nicolay, former intern in BDI's Brussels Office, who conducted a survey on US cybersecurity policy and its implications for German businesses.