THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE

SciencesPo
Paris School of International Affairs
Technology & Global Affairs
INNOVATION HUB

Defragmenting international cybersecurity regulations

Alexander Evans & Pierre Noro

London School of Economics & Sciences Po

April 2026

The authors

Alexander Evans is a Professor in Practice and Associate Dean at the London School of Economics School of Public Policy where he researches and teaches on technology and geopolitics. He was formerly an adviser to the Prime Minister in 10 Downing Street, Strategy Director in the Cabinet Office and Director Cyber in the UK Foreign Office.

Pierre Noro is Adjunct Faculty member at Sciences Po Paris and Université Paris-Cité, and an Advisor to the Sciences Po Paris School of International Affairs Tech & Global Affairs Hub. His work is dedicated to tech governance and digital ethics, with a focus on the evaluation and improvement of digital technologies' social and environmental impacts.

This paper draws on a Sciences Po / London School of Economics on The Future of Cybersecurity Regulations held in Paris in November 2025 as well as interviews and research with cybersecurity regulators, industry experts and academics. The authors are grateful to Microsoft for their support.

Contents

Executive Summary

Improving cybersecurity regulations

1 The future of cybersecurity regulations

2 Improving cybersecurity regulations

3 The cybersecurity threat

4 Aligning cybersecurity reporting

5 Mutual recognition as a tool for harmonisation

6 Case-study: Singapore and South Korea

7 Harnessing the broader momentum for mutual recognition

8 Case-study: The European Union and the United States

9 A role for the OECD?

Forming the Future

Executive summary

Cyber-attacks place growing costs on citizens, business and government. Investing more in cybersecurity is an international priority, but one that needs to support economic growth, national security and global stability – a core agenda for all governments. Yet cybersecurity regulation is becoming more fragmented within individual countries as well as across borders, despite the reality that cyber threats don't respect sectoral or national boundaries.

Medium and large companies face a complex array of cybersecurity incident reporting and compliance standards, many of which vary and some of which are inconsistent with each other (even when reporting incidents within a single country). This impedes economic growth, diverts resources to duplicative or unnecessary compliance, disrupts early-detection of and appropriate response to emerging threats, complicates setting clear, common standards and reduces funding to invest in frontline cybersecurity.

Even in a more sovereignty-driven world where trade policy, security and other international differences complicate cooperation, with AI technologies set to dramatically accelerate threats[1], the need for purposeful regulatory defragmentation is becoming more – not less – important. This applies at both the national and international level.

Too often, discussions about cybersecurity happen in sectoral verticals, national silos, or within a single regulatory body. They fail to identify converging interests between stakeholders which benefit from cybersecurity as a common good. This policy paper from the London School of Economics and Sciences Po provides a practical analysis of feasible interventions on which past approaches have demonstrated measurable impact.

Simplifying and aligning cybersecurity incident reporting is one obvious pathway, with the added benefit of improving the quality and speed of reporting while reducing error rates.

Identifying avenues for mutual recognition of regulations or standards – as South Korea and Singapore did in 2025[2] – is another practical step. It advances cyber cooperation, creates legal clarity and operational alignment without compromising national sovereignty or standard-setting.

Among the institutions able to host this debate, the OECD is prominently positioned. On top of its ongoing working party on digital security, it has a track-record of facilitating reforms, like tax regulatory standards, as vectors of economic growth and social

[1] See Anthropic. (2025, November 17). *Disrupting the first reported AI-orchestrated cyber espionage campaign* and Heelan, S. (2026, January 18). On the coming industrialisation of exploit generation with LLMs. *Sean Heelan's Blog*. https://sean.heelan.io/2026/01/18/on-the-coming-industrialisation-of-exploit-generation-with-llms/

[2] See Digital Policy Alert. (2025). *Republic of Korea: Implemented Singapore – Korea mutual recognition agreement for recognition of cybersecurity labels*; Cyber Security Agency of Singapore. (2024, October 16). *Singapore signs mutual recognition arrangements with Republic of Korea and Germany on cybersecurity labelling for consumer smart products*.

progress.[3] It understands the important yet technical work that underpins simplification (e.g. forms, processes, communication channels), standards discussions and mutual recognition.

The scale of the challenge and the need to boost cybersecurity for the super-priority of economic growth and global stability requires nonetheless a different, broader conversation. A new regular forum (potentially in collaboration with the OECD, such as the one co-hosted by Sciences Po and the London School of Economics in November 2025)[4] could play a catalytic role in gathering regulators, government decisionmakers, experts and industry from the entire world in a neutral but purposeful space to share best practices but more importantly to stimulate and scale practical initiatives that demonstrate the benefit of simplification and mutual recognition.

[3] See Hernandez Gonzalez-Barreda, P. A. (2018). A historical analysis of the BEPS Action Plan: Old acquaintances, new friends and the need for a new approach. *Intertax*, *46*(4), 278–295; OECD. (2002). *Regulatory policies in OECD countries: From interventionism to regulatory governance*.

[4] Sciences Po and the London School of Economics (LSE) organized an event immediately following an OECD Working Party meeting in November 2025. This event convened cybersecurity regulators from OECD countries, industry leaders, and academics as a proof-of-concept for a regular OECD-led meeting series on regulatory alignment.

Improving cybersecurity regulations

1. The future of cybersecurity regulations

In November 2025, Sciences Po along with the London School of Economics (LSE) and Business at the OECD (BIAC) hosted a workshop in Paris on The Future of Cybersecurity Regulations, building on an earlier gathering held in the United Kingdom in September 2024.

The Paris event brought together regulators from OECD member countries, industry leaders, and academic experts under the Chatham House rule to compare cybersecurity regulations across jurisdictions, identify commonalities and conflicting norms, and explore opportunities for greater coordination.

Participants examined how the rapid proliferation of national cybersecurity frameworks, although positively fostering greater security, has created increasing fragmentation and complexity. Expanding the coverage and protection of generally shared principles and influential policies, this regulatory inflation has come at a significant financial and operational cost for cross-border organizations and businesses. Regulators and experts shared their perspectives on the near future of cyber defense and outlined actionable public-private collaboration approaches to prevent these well-intentioned legal frameworks from the EU's NIS2 to the African Malabo Convention from becoming counter-effective.

The session served as a proof-of-concept for establishing regular dialogue on cybersecurity regulations through the OECD framework. These discussions have stimulated this paper, which draws on insights from the event and a range of applied research to examine how regulatory coordination can reduce costs and errors around compliance while making security protections more robust. It also assesses the OECD's potential role in tracking best practices, developing consensus, and advancing harmonization, mutual recognition, and simplification of cybersecurity regulatory requirements across borders.

2. Improving cybersecurity regulations

Economic growth and national security have emerged as the superpriority for governments worldwide in 2026 as states confront sluggish productivity, fiscal pressures, and heightened geopolitical competition.[5] Countries across the OECD face mounting pressure to boost innovation, accelerate investment, and remove barriers that limit business expansion. Yet cybersecurity incidents directly undermine these growth objectives. According to IBM research, the average data breach now requires 241 days

[5] See Kammer, A. (2025, September 20). *National-level priorities to lift growth in the EU: Why, what, and how?* [Background note prepared for the EU's Economic and Financial Affairs Council (ECOFIN)]. International Monetary Fund; International Monetary Fund. (2026, January 19). *World Economic Outlook Update, January 2026: Global economy: Steady amid divergent forces*.

to be detected,[6] creating extended periods of operational disruption that suppress the target organization's productivity and divert its resources from growth-generating activities, a delay during which all its stakeholders (partners, employees, customers) are also exposed.

Governments' ability to track, monitor, and compare cybersecurity incidents as well as campaigns by malicious cyber threat actors are hindered by diverging definitions and requirements. Unaligned or duplicative regulations increase the resources required by governments to effectively implement them. This moves the focus away from boosting cybersecurity or national security priorities and generates unnecessary costs. There is a longstanding problem of shortages of cybersecurity staff and expertise[7] which persists.[8] This is about both a lack of qualified experts to fill jobs and the challenge of finding candidates with the right skills match. In 2024 more than half of European companies for example reported difficulties in finding the right candidate.[9]

Compliance costs compound these challenges. Organizations increasingly confront plural, competing, and sometimes contradictory cybersecurity reporting requirements across jurisdictions, with companies operating in multiple European markets facing up to 27 separate compliance frameworks under NIS2 alone despite the directive's ostensibly harmonized objectives.[10] NIS2 is a directive, not a regulation, so each of the 27 member states transposes it into its own national law. By mid-2025 only 14 of 27 states had fully transposed, and those that have done so have produced varying national requirements despite the shared intent of NIS2.[11]

This regulatory fragmentation forces businesses to maintain separate compliance teams (or sometimes rely on local contractors), duplicate (and vary) their reporting efforts, and navigate inconsistent interpretations of fundamentally similar security obligations. The result drags on economic performance without improving cybersecurity, generating friction rather than the goal of coordinated regulation.

> *If national or cross-European Union consistency is one problem, international consistency is another.*

---

[6] IBM. (2025). *Cost of a Data Breach Report 2025*. IBM Security / Ponemon Institute. https://www.ibm.com/reports/data-breach

[7] See OECD. (2023). *Building a skilled cyber security workforce in five countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States*.

[8] ISC2. (2025). *2025 ISC2 cybersecurity workforce study*. ISC2.

[9] European Commission. (2024). *Flash Eurobarometer 547: Cyberskills*. Directorate-General for Communications Networks, Content and Technology. https://europa.eu/eurobarometer/surveys/detail/3176

[10] This is well evidenced, including from the EU's own reporting. European Cyber Security Organisation. (2025). *NIS2 Directive transposition tracker*. ECSO; Skadden, Arps, Slate, Meagher & Flom LLP. (2025, August). *NIS2 update: EU cyber authority sets out compliance expectations, but implementation is a work in progress*.

[11] FTI Consulting. (2025, August 8). *NIS2 – Implementation of the Second Directive*.

As mentioned during the event: "If national or cross-European Union consistency is one problem, international consistency is another." Most medium and large companies operate across borders, and so do small digital businesses servicing customers in many different countries without having local offices or staff. Interacting with multiple national authorities to comply with different reporting requirements, timelines, forms or even formats is a necessary but expensive byproduct of the current fragmented, high-friction regulatory environment. Errors and compliance costs go up, eating into the investment so badly needed for better underlying cybersecurity capabilities and infrastructure.

3. The cybersecurity threat

Over the past eighteen months the cybersecurity threat has once again come into focus. Salt Typhoon, an advanced state-linked cyber-attack was found to have penetrated organisations in more than 80 countries, including infiltrating the networks of at least nine major US telecoms companies, including AT&T and Verizon.[12] A major ransomware attack in the United Kingdom directed against Marks and Spencer ended up costing the company some £300m.[13] In November 2025, Salesforce disclosed that hackers had accessed customer data through apps published by Gainsight, a customer success platform – a major data breach.[14] Meanwhile DDOS attacks sharply increased during 2025 according to Cloudflare. The Aisuru-Kimwolf botnet launched what was dubbed "The Night Before Christmas" campaign, targeting Cloudflare customers and infrastructure with HTTP DDoS attacks exceeding 200 million requests per second.[15] A separate single attack in Q4 peaked at 31.4 terabits per second, lasting just 35 seconds, and hyper-volumetric attacks grew by over 700% compared to large attacks seen in late 2024.[16]

The cost of fragmentation is especially concerning in a context of expanding global cybersecurity threats, with more capable Artificial Intelligence (AI) systems able to autonomously scan, test, and exploit vulnerabilities, lowering the barriers to scaled-up cyber attacks and exposing citizens, businesses, and governments worldwide to staggering costs.[17] Cybercrime has become an economic force rivaling the world's largest economies, with projected annual costs reaching $10.5 trillion in 2025.[18] This equals the third-largest economy globally, trailing only the United States and China. The

---

[12] Krouse, S., McMillan, R., & Volz, D. (2024, September 26). China-linked hackers breach U.S. internet providers in new 'Salt Typhoon' cyberattack. *The Wall Street Journal*.
[13] Tidy, J. (2025, May 13). M&S says personal customer data stolen in recent cyber attack. *BBC News*. https://www.bbc.co.uk/news/articles/c62v34zv828o
[14] Franceschi-Bicchierai, L. (2025, November 21). Google says hackers stole data from 200 companies following Gainsight breach. *TechCrunch*. https://techcrunch.com/2025/11/21/google-says-hackers-stole-data-from-200-companies-following-gainsight-breach/
[15] Yoachimik, O., Pacheco, J., & Cloudforce One. (2026, February 5). 2025 Q4 DDoS threat report: A record-setting 31.4 Tbps attack caps a year of massive DDoS assaults. *The Cloudflare Blog*. https://blog.cloudflare.com/ddos-threat-report-2025-q4/
[16] Ibid
[17] See Sean Heelan, "On the Coming Industrialisation of Exploit Generation with LLMs" (January 18, 2026) or Anthropic "Disrupting the first reported AI-orchestrated cyber espionage campaign" (November 2025)
[18] See Deep Strike, "Cybersecurity Statistics 2025: Key Trends & Breach Costs" (November 29, 2025)

figure marks a 31% rise in 2024, with ransomware a particular factor.

The average cost of data breaches grew for US organisations, jumping 9 percent to a record $10.22 million (driven by higher regulatory fines and detection and escalation costs). Healthcare remained the costliest sector for the fourteenth consecutive year at $7.42 million per incident. On average, organisations took 241 days to identify and contain a breach — the lowest figure in nine years, but still long enough for attackers to implant malware, especially ransomware, and exfiltrate sensitive data. [19]

Ransomware attacks have surged dramatically. Over 5,400 disclosed attacks targeted organizations in 2024, with ransomware present in 44 percent of all breaches, up from 32 percent previously. According to Sophos research across 17 countries and 3,400 organisations, the average ransom payout in 2025 was $1m.[20] Meanwhile many organizations still refuse to disclose falling victim to attacks: roughly two-thirds of UK businesses that experienced a breach did not report it to any outside body.[21]
Small and medium-sized enterprises (SME) bear a disproportionate burden. Ransomware featured in 88 percent of SME breaches, far outstripping the rate for larger firms. A Mastercard survey of over 5,000 SME owners found that nearly one in five of those suffering a cyber-attack filed for bankruptcy or closed entirely.[22]

The human factor remains stubborn: 60 percent of all breaches involved phishing, social engineering, or errors. Third-party involvement doubled from 15 to 30 percent of breaches, driven by software vulnerabilities, partner credential exposures, and misconfigured cloud environments.[23] The cascading effects of single-vendor compromises demand coordinated regulatory approaches that reduce compliance friction and enable synchronised cybersecurity responses.

4. Aligning cyber-incident reporting

Boosting cybersecurity is a team sport. As experts at the LSE/Sciences Po meeting in Paris pointed out, only by sharing incident reports and threat information, specific tradecraft, signatures and trends can the cybersecurity community, from specialized companies to government agencies track trends and mutualize defensive efforts. This depends on effective incident reporting, frequently – though not always – formally mandated by regulators. This is particularly crucial in high-risk industries from nuclear energy to healthcare and financial services where the effects of multiple regulatory reporting requirements could ultimately undermine safety.

---

[19] See IBM, Cost of a Data Breach Report 2025
[20] Sophos. (2025, June). *The state of ransomware 2025*. https://www.sophos.com/en-us/content/state-of-ransomware
[21] Department for Science, Innovation and Technology & Home Office. (2025, April 1). *Cyber security breaches survey 2025*. GOV.UK. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025
[22] Mastercard. (2025, April 23). *Small business cybersecurity: Survey shows reason for worry*. https://www.mastercard.com/us/en/news-and-trends/stories/2025/small-business-cybersecurity-study.html
[23] Verizon. (2025, April 23). *2025 Data Breach Investigations Report*. https://www.verizon.com/business/resources/reports/dbir/

"Boosting cybersecurity relies on effective incident reporting."

As data and digital services increasingly underpin national infrastructure, the attack surface is now everywhere. This in turn involves a greater number of national regulators, standards and reporting obligations. This can result in a "regulatory paella" with differing ingredients and recipes depending on which sector or country one operates in. But every variant requires one essential ingredient: a reporting form. These forms vary enormously in type, format, fields and timelines. Cyber incident reporting has become the challenge of 'everything, everywhere, all at once' with rising threats and ever more complex reporting requirements.

The need for greater alignment in cyber incident reporting proved to be a key insight from the Sciences Po/LSE event, both for practical and strategic reasons. As an initial focus for reform this tackles one of the most complex and burdensome areas for industry and regulators, where improved alignment would deliver immediate benefits. Due to the existing lack of standardization, aligning definitions, timelines, and thresholds would reduce duplicative compliance efforts, free critical cybersecurity talent, and enable faster, coordinated responses. There is a security and economic dividend from this, both at the national and global levels. Standardizing reporting requirements would provide a foundation for broader coherence, paving the way for reciprocity agreements and mutual recognition frameworks. While incident reporting is a critical starting point, there are numerous other areas within cybersecurity regulations that necessitate greater alignment and further research.

This is where the academic Cass Sunstein's work is relevant. He is the Robert Walmsley University Professor at Harvard Law School and widely regarded as one of the most influential scholars of regulation and behavioural economics. He is best known for co-authoring *Nudge* (2008)[24] with Richard Thaler. He later coined the term 'sludge', defining forms of bureaucratic friction. At the Paris meeting participants returned repeatedly to the challenge of friction in regulatory reporting, which industry participants assessed to be a growing problem. Plural, duplicative and varying (and sometimes contradictory) reporting requirements make boosting cybersecurity challenging.

As they pointed out, forms that demand duplicative information, varying reporting deadlines, and templates that differ across regulators for fundamentally identical incidents all constitute friction that wastes resources while degrading the quality of information collected. This is not limited to cybersecurity: in 2015, the United States government imposed an estimated 9.78 billion hours of paperwork on Americans.[25] Much of this burden stems not from what information regulators seek but how they ask for it. The causes of this are broader than the challenge of cybersecurity regulation, but the consequences are similar.

---

[24] Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

[25] Sunstein, C. R. (2019). Sludge and ordeals. *Duke Law Journal*, *68*(8), 1843–1883. https://scholarship.law.duke.edu/dlj/vol68/iss8/6/

> *Regulatory duplication already multiplies within as well as across national borders.*

The problem is most acute when organizations must report the same incident to multiple regulators using different forms with different deadlines. Europe provides the clearest example. Under current frameworks, a cybersecurity incident may require reporting under NIS2, the Cyber Resilience Act, and the General Data Protection Regulation.[26] Each regulation introduces distinct definitions, thresholds, timelines, and content requirements. Companies face the burden of adapting essentially identical information about what happened into multiple formats to satisfy different legal requirements. The GDPR alone generated 132,000 breach notifications in 2024.[27] Data breaches may also trigger NIS2 reporting obligations, further duplicating effort.
This duplication multiplies within countries as well as across borders. Whether a cybersecurity incident affects individuals across different countries or a single critical infrastructure, it often requires separate notifications to data protection authorities, sector regulators, and national security agencies. Each authority requests overlapping information through distinct proprietary forms with uncoordinated deadlines. Regulated entities either maintain separate or larger compliance teams to manage these parallel obligations.

Take two examples of how this can apply in practice:

- A single breach at an EU-based bank could require: a DORA initial notification to the financial supervisor within 4 hours of classifying the incident as major (and no later than 24 hours of becoming aware of it); a NIS2 early warning to the national CSIRT within 24 hours; and a GDPR personal data breach notification to the data protection authority within 72 hours.[28]
- A ransomware attack on a publicly traded US hospital could trigger: a CIRCIA covered cyber incident report to CISA within 72 hours, plus a separate ransomware payment report within 24 hours; an SEC public disclosure on Form 8-K within four business days of determining materiality; a HIPAA breach notification to HHS within 60 calendar days if 500 or more patients are affected; and notification to one or more state attorneys general under the relevant state breach notification statutes, with deadlines ranging from 30 to 90 days depending on the jurisdiction.[29]

---

[26] Houston, L., Jeens, R., Burns, C., & Donovan, N. (2025). *EU proposes single-entry point for cyber incident reporting, but is it really "report once, share many"?* Slaughter and May. https://thelens.slaughterandmay.com/post/102lxgd/eu-proposes-single-entry-point-for-cyber-incident-reporting-but-is-it-really-re

[27] DLA Piper. (2025, January). *GDPR fines and data breach survey: January 2025*. https://www.dlapiper.com/en-gl/insights/publications/2025/01/dla-piper-gdpr-fines-and-data-breach-survey-january-2025

[28] See Bird & Bird. (2025). Digital Omnibus package: Single EU harmonised incident reporting regime across cyber and data protection. https://www.twobirds.com/en/insights/2025/digital-omnibus-package-single-eu-harmonised-incident-reporting-regime-across-cyber-and-data-protect

[29] See U.S. Government Accountability Office. (2025, July 30). *Cybersecurity regulations: Industry perspectives on the impact, progress, challenges, and opportunities of harmonization* (GAO-25-108436).

> *As AI will increasingly be used to examine and interrogate incident reporting, the consistency and accuracy of that data become more important.*

As one regulator at the Paris meeting noted, these standards impose different reporting requirements and timelines for what is in essence the same event. Unsurprisingly companies want standardized reporting timelines and formats rather than managing multiple forms. But there is also a utility for regulators and governments from consistent incident reporting requirements. As AI will increasingly be used to examine and interrogate incident reporting, the consistency and accuracy of that data become more important. Even if there is scope for regulators to use AI to better investigate and correlate reports, the burden will still fall on companies to fulfil reporting requirements. Against a complex and changing threat picture, where AI tools will be used to increase the scale of attacks, it becomes critical for regulators and cybersecurity actors to have a single version of the truth in terms of reported cyber security incidents to identify weak signals indicating the emergence of new threats and respond as fast as possible in a coordinated manner.

Form design itself creates unnecessary friction. Sunstein emphasizes that radical simplification and plain language can eliminate learning costs while improving compliance.[30] Yet many reporting forms are either unnecessarily complex or lack essential UX design principles reflecting how the reporting is generated and most likely to be used. Even with different legal parameters, they may follow unnecessarily different models across jurisdictions to capture substantially the same information, making fast transposition of reports arduous. Some of this may derive from primary legislation or regulations and it is true that revising these may prove more challenging. But most reporting forms are layered over the underlying legislation or regulation and there is flexibility for regulators to simplify, standardise and make machine-readable where appropriate.

> *Simplifying incident reporting is a low-hanging fruit.*

When this does not happen – as is mostly the case - fields fail to align with how organizations naturally track and store information. Internal company staff translate internal data into regulatory formats. This translation introduces errors and consumes time (and resources) that could be spent on substantive compliance, when it does not outright deter small businesses from reporting incidents altogether, although 46% of them would have already experienced a cyberattack.[31] This is why work on simplifying incident reporting is a low-hanging fruit. It can be done by individual regulators as well as collectively, with the latter generating the greatest efficiency dividend.

First, regulators need harmonized incident thresholds. When one framework defines a significant incident based on number of affected users while another uses service

https://www.gao.gov/products/gao-25-108436

[30] Thaler, R. H., & Sunstein, C. R. (2008). *Nudge: Improving decisions about health, wealth, and happiness*. Yale University Press.

[31] Based on a survey on 5000+ SMEs, Mastercard white paper "SME Cybersecurity Part 1" October 2025

disruption duration, companies must conduct parallel assessments for the same event. Harmonizing thresholds around common measures allows a single assessment to satisfy multiple requirements.

Second, aligned timelines dramatically reduce compliance burden. The GDPR established a 72-hour reporting window. If other frameworks mandate immediate notifications, 24-hour (e.g. the EU's NIS 2 directive) or 6-hour (e.g. India's CERT-In directions) deadlines, companies then need to maintain systems capable of producing multiple reports to different schedules. Aligning to a common timed window for initial notification may seem pedestrian but it would likely again make reporting easier without degrading the quality. Under Article 33 of GDPR, organizations must notify the relevant supervisory authority "without undue delay and, where feasible, not later than 72 hours after having become aware of" a personal data breach.[32] This 72-hour timeline has become a model that other cybersecurity regulations reference. This timeline allows non-critical organizations sufficient time to verify the incident, assess its impact, and gather essential details before notification. This is why it's being proposed as a harmonized standard across NIS2, the Cyber Resilience Act, and other EU cybersecurity frameworks. But this move by the EU to systematise is still relatively rare: most incident reporting requirements vary. Reporting requirements within the United States illustrate this, varying from one hour to four business days: one hour for federal agency reporting to CISA, FedRAMP, DOD CC SRG, VAAR, and NERC CIP-008; 24 hours for TSA pipeline and rail security directives; 72 hours for CIRCIA, DFARS, and NCUA rules; and four business days for the SEC disclosure rule.[33]

Third, standardized templates eliminate friction. A single harmonized machine-readable form containing core fields applicable across regulations improves the fidelity of reports and reduces the compliance burden. Essential elements include incident description, impact assessment, mitigation measures, and follow-up actions. A 'base form' for incident reporting does not preclude optional fields to accommodate sector-specific requirements or, when pertinent, national variations.

One further possible step is to have a single point of contact or reporting for multiple regulators, allowing single reporting through unified channels. A one-stop shop platform managed centrally but with automatic routing to relevant authorities could be another efficiency – and again has potential in an environment where the move to AI-interrogated data lakes depends on aggregated, interoperable data. Access to anonymized datasets from these data lakes could also enable new cybersecurity research and forensics operations, at both national and international levels.

The European Union's single reporting platform under the Cyber Resilience Act could be used as a foundation.[34] Strengthening this platform to cover all relevant regulations would consolidate incident reporting through one entry point. This is a larger regulatory

[32] Regulation 2016/679. *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)*.
[33] Department of Homeland Security, Cyber Incident Reporting Council. (2023, September). *Harmonization of cyber incident reporting to the Federal Government*.
[34] Regulation 2024/2847. *Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) No 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)*.

reform task than simplifying forms or fostering specific mutual recognition agreements, but as a medium-term aspiration it would set a signal for wider regulatory policies.

> *Smaller companies and organisations suffer disproportionately from duplicative reporting requirements.*

There is a huge potential dividend for small and medium-sized companies: often the engine for employment and economic growth. Smaller companies lack dedicated compliance teams and suffer disproportionately from duplicative reporting requirements.

Form simplification delivers measurable benefits. Organizations can spend less time on compliance. Information quality improves when forms request information clearly (and error is a specific challenge for regulatory reporting and action). Regulatory effectiveness increases when authorities receive timely, accurate reports through coordinated systems. The path forward requires coordination among regulators to harmonize thresholds, align timelines, and standardize templates. Without this alignment, regulatory fragmentation will accumulate at the expense of cybersecurity and economic growth. A key recommendation is the importance of following internationally recognized cybersecurity standards and frameworks because they reduce fragmentation and conflicting requirements, enabling governments and industry to implement consistent, risk-based security measures across borders. Moreover, adopting shared standards also streamlines compliance, lowers operational complexity, and strengthens global cyber defences by creating a coherent foundation for reciprocity, mutual recognition, and coordinated response to cross-border threats.

5. Mutual recognition as a tool for harmonization

The principle of mutual recognition is not new. In the nineteenth century emerging technologies like railways and the telegraph system depended on integrated national standards and cross-border agreement on international standards or mutual recognition.[35] In the twentieth century this increasingly extended to diplomas[36] and professional credentials, as for example allowing selected medical doctors to have their original medical degrees recognised as equivalent in other jurisdictions.[37] The OECD and the EU played a significant role in deepening the practice. Mutual recognition emerged as a powerful mechanism, especially when the pursuit of full harmonization initially failed (as it did for medical doctors qualifications within Europe).[38] Automatic recognition was eventually introduced in 2005.[39] Best of all, it permits both sovereignty – preserving national regulatory autonomy, sometimes a keen political issue (as for example with food standards) while allowing mutual recognition, a degree of interoperability and

[35] Puffert, D. J. (2009). *Tracks across continents, paths through history: The economic dynamics of standardization in railway gauge*. University of Chicago Press; Headrick, D. R. (1991). *The invisible weapon: Telecommunications and international politics, 1851–1945*. Oxford University Press.
[36] Such as the European Credit Transfer and Accumulation System (ECTS), a cornerstone of the European Higher Education Area initiated by the Bologna Declaration of 1999.
[37] Karle, H. (2008). International recognition of basic medical education programmes. *Medical Education*, *42*(1), 12–17.
[38] Nicolaïdis, K., & Shaffer, G. (2005). Transnational mutual recognition regimes: Governance without global government. *Law and Contemporary Problems*, *68*(3–4), 263–317.
[39] See Directive 2005/36/EC of Sep 7 2005

market access.

In the digital field, the GDPR provides an interesting example of mutual recognition that can serve as a source of inspiration for cybersecurity regulators. In Article 45, the GDPR grants the European Commission the power to adopt, with the visa of the European Data Protection Board, an "adequacy decision" recognizing that a third country provides data protection equivalent to the European legislation and identifying the local supervisory authority.[40] Thanks to this mutual recognition mechanism, European data can thus be transferred to 16 countries without additional safeguards, as it would flow between member states. A similar scheme could easily be implemented for cybersecurity regulations, starting with incident notification with public authorities recognizing equivalent foreign institutions equipped with the reception, initial treatment, and communication of a single standardized report, before being extended to other aspects of cyber regulation. Assessing the economic benefits of mutual recognition is methodologically challenging. However, the costs of losing such frameworks are evident. For example when the Court of Justice of the EU struck down the EU US "Privacy Shield" adequacy decision and forced companies to reevaluate their Standard Contractual Clauses (SCCs), only half of the companies initially complied.92% of them declared that the reassessment came at moderate or high cost.[41]

One advantage of mutual recognition agreements is that bilateral agreements can be driven, delivered, and revised at pace. This is well illustrated by the 2025 Singapore – South Korea agreement explained below.

6. Case-study: Singapore and South Korea

Singapore and South Korea implemented a mutual recognition arrangement for cybersecurity labels on 1 January 2025.[42] This groundbreaking arrangement strengthens trust in certified smart consumer products and aligns the cybersecurity evaluation systems of both countries.

Singapore's Cyber Security Agency and the Korea Internet and Security Agency drove this agenda. The agencies accept each other's labels for smart home assistants, IoT gateways and similar devices. Manufacturers benefit from quicker access to both markets. They can avoid redundant testing and reduce compliance costs. The advantage is that consumers gain clearer information about the security of connected devices.

KISA's basic level certification meets Singapore's Cybersecurity Labelling Scheme Level 3 requirements. This level indicates that developers follow security by design and show that third party laboratories have assessed software binaries. These shared standards help both countries promote safer digital ecosystems.

[40] Kuner, C. (2020). Article 45: Transfers on the basis of an adequacy decision. In C. Kuner, L. A. Bygrave, C. Docksey, & L. Tosoni (Eds.), *The EU General Data Protection Regulation (GDPR): A commentary* (pp. 782–804). Oxford University Press.
[41] See Digital Europe, Business Europe, ERT and ACEA (2020) *Schrems II, Impact Survey Report*.
[42] See Digital Policy Alert. (2025). *Republic of Korea: Implemented Singapore – Korea mutual recognition agreement for recognition of cybersecurity labels*; Cyber Security Agency of Singapore. (2024, October 16). *Singapore signs mutual recognition arrangements with Republic of Korea and Germany on cybersecurity labelling for consumer smart products*.

The agreement originated from efforts to harmonize digital product standards. Agencies formalized the arrangement on 16 October 2024 and it was formally launched on 1 January 2025. This timeline demonstrates what is possible in a relatively short timeline through bilateral digital cooperation, supporting long term collaboration in cybersecurity regulation.

Both countries aim to support innovation without lowering safety requirements, encouraging manufacturers to adopt stronger cybersecurity practices. They also help consumers make informed choices when buying connected devices. This agreement strategically reinforces trust in cross border digital trade: Singapore and South Korea were each other's seventh largest export partner in 2024, with electronic equipment being a top category on both sides.[43] It remains to be seen if the mutual recognition agreement will further reinforce the current momentum between the two economies (since 2019, their mutual trade flows in electronic goods and in telecommunication services have respectively doubled and tripled).[44] In any case, it already improves regulatory efficiency, lowering costs for businesses in a highly competitive global market, while still signaling a commitment to shared cybersecurity goals.

> *South Korea and Singapore demonstrate what is possible in a relatively short timeline through bilateral digital cooperation.*

7. Harnessing the broader momentum for mutual recognition

There are continuing efforts across different sectors to reach mutual recognition agreements, with noteworthy movement within the African Union, Association of Southeast Asian Nations (ASEAN), by Canada and the European Union. Although it is often a slower process to land specific regional or multilateral mutual recognition agreements, there is scope for these to be achieved regionally (the EU is one example) and ASEAN has also shown commitment to this regulatory policy agenda.

Initially adopted in 2014, the African Union convention on cyber security and personal data protection, known as the "Malabo Convention", lays the groundwork for the establishment of cybersecurity authorities and legislation in each member states. Article 28 of the convention mandates signatories to ensure harmonization, information exchange and mutual assistance in fighting cyber-crime.[45] Charting an ambitious roadmap, the legal framework only came into force in 2023 and is binding in the 16 member states which ratified the convention.[46]

[43] According to the United Nations COMTRADE database on international trade.
[44] Ibid, from USD 7.31B to USD 13.02B in 2024 for electrical and electronics (HS 85) and from USD 0.387B to USD 1.216B in 2023 for telecommunications, computer and information services (EBOPS 9).
[45] See the African Union Convention on Cyber Security and Personal Data Protection
[46] The ratifiers are Angola, Cape Verde, Congo, Ghana, Guinea, Mauritania, Mozambique, Namibia, Niger, Rwanda, Senegal, Sao Tome and Principe, Togo, Zambia, Côte d'Ivoire & Mauritius.

More recently, in February 2025, all ten ASEAN Member States of Brunei Darussalam, Cambodia, Indonesia, Laos, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam signed the ASEAN Framework Agreement on Mutual Recognition Arrangements in Vientiane. They created a shared structure that helps these governments recognise each other's conformity assessment bodies. The agreement aims to reduce technical trade barriers and support a more integrated regional economy by aligning procedures for testing, inspection and certification. It encourages smoother movement of regulated goods across the ASEAN region and strengthens trust in product quality standards.[47]

Several Asia Pacific economies also participate in the Asia-Pacific Economic Cooperation (APEC) Mutual Recognition Arrangement for Conformity Assessment of Telecommunications Equipment. The arrangement applies when two or more APEC governments agree to recognise each other's testing and certification results. Economies such as Australia, Canada, Chile, China, Hong Kong, Japan, Malaysia, Mexico, New Zealand, Peru, Singapore, South Korea, Chinese Taipei, Thailand, the United States and Vietnam can participate when they opt in. The arrangement helps manufacturers reduce delays and comply with technical regulations more easily because the importing country accepts test reports from the exporting economy's recognised bodies. It strengthens regional trade by creating predictable and efficient regulatory processes for telecommunications products. [48]

Canada maintains a set of Mutual Recognition Arrangements for telecommunications equipment with several partners, including APEC economies, the European Free Trade Association states of Iceland, Liechtenstein and Norway, the European Union, the United Kingdom, Switzerland, Mexico and Israel.[49] These arrangements permit the mutual acceptance of conformity assessment procedures, which simplifies entry into foreign markets for Canadian manufacturers. They reduce the need for repeated testing in multiple jurisdictions and help trading partners coordinate regulatory frameworks. Canada updates these arrangements to stay aligned with international technical requirements.

Beyond the tech sector, mutual recognition works in other areas like medicines. The European Union and governments including the United States, Australia, Canada, Switzerland, New Zealand, Israel and Japan participate in Mutual Recognition Agreements covering Good Manufacturing Practice inspections for medicines.[50] These agreements allow regulators to rely on each other's inspections and waive duplicate batch testing for imported pharmaceuticals. They support public health authorities by freeing inspection resources for higher risk facilities and reducing compliance costs for

---

[47] Association of Southeast Asian Nations. (2025). *ASEAN Framework Agreement on Mutual Recognition Arrangements*. ASEAN Secretariat. https://asean.org/asean-framework-agreement-on-mutual-recognition-arrangements/

[48] Asia-Pacific Economic Cooperation. (1998, May 8). *Mutual Recognition Arrangement for Conformity Assessment of Telecommunications Equipment*. https://www.apec.org/groups/som-steering-committee-on-economic-and-technical-cooperation/working-groups/telecommunications-and-information/apec_tel-mra

[49] Innovation, Science and Economic Development Canada. (n.d.). *Agreements/Arrangements: Mutual Recognition Agreements/Arrangements*. Government of Canada. Retrieved March 23, 2026, from https://ised-isde.canada.ca/site/mutual-recognition-agreements/en/agreements-arrangements

[50] European Medicines Agency. (n.d.). *Mutual recognition agreements (MRA)*. Retrieved March 23, 2026, from https://www.ema.europa.eu/en/human-regulatory-overview/research-development/compliance-research-development/good-manufacturing-practice/mutual-recognition-agreements-mra

manufacturers.

Despite a complicated international geopolitical environment and the renewed use of tariffs as part of economic (and wider) negotiations, regional or bilateral mutual recognition agreements are realistic tools to advance regulatory convergence. Despite tensions, the EU and the United States have also signalled intent on mutual recognition.[51] Progress since original commitments were made in 1998 has been slow, but the fact that the ambition remains on the table in 2025 – despite challenging political times – is a positive signal.

> *As the global economy tilts to become data and digital-services dependent the potential economic value of progressing mutual recognition grows.*

The experiences above speak to the potential to embed mutual recognition into bilateral and multilateral agreements, all the while protecting red lines on national sovereignty and standards. As the global economy tilts to become data and digital-services dependent, including for 'real world' services like logistics, government and healthcare, the potential economic value of progressing mutual recognition grows. There is also potential competitive economic value for early adopters, which is why the South Korea – Singapore agreement is so interesting.

8. Case-study: The European Union and the United States

The 2025 Framework on an Agreement on Reciprocal, Fair, and Balanced Trade between the United States and the European Union was announced on 21 August 2025.[52] It presents itself as a renewed foundation for transatlantic economic cooperation and describes its purpose as a "concrete demonstration of our commitment to fair, balanced, and mutually beneficial trade and investment."[53] Although it does not formally replace the 1998 Mutual Recognition Agreement on conformity assessment, it is more ambitious.

The 2025 framework states that the United States and the European Union "intend to accept and provide mutual recognition to each other's standards," a broader and more forward leaning commitment that suggests interest in recognising not only assessment results but also the standards that underpin them.[54] It also highlights plans to expand recognition across additional industrial sectors and to strengthen technical cooperation between standards bodies. The avoidance of duplication also appears more prominently.

[51] See White House and European Commission (2025, August 21). *Joint Statement on a United States–European Union Framework on an Agreement on Reciprocal, Fair, and Balanced Trade*.
[52] White House and European Commission (2025, August 21). *Joint Statement on a United States–European Union Framework on an Agreement on Reciprocal, Fair, and Balanced Trade*.
[53] White House and European Commission. (2025, August 21). *Joint statement on a United States–European Union framework agreement on reciprocal, fair and balanced trade.*
[54] Ibid, and see Cripps, S. B., McElwee, M., Bartels, L., & Carr, C. (2025, August 27). The EU–US trade framework: The battle continues. Freshfields Bruckhaus Deringer Risk & Compliance Blog. https://riskandcompliance.freshfields.com/post/102l2ww/the-eu-us-trade-framework-the-battle-continues

It includes commitments to streamline processes and address technical barriers that cause unnecessary compliance burdens.[55]

Paragraph 13 of the agreement commits the United States and the European Union to "negotiate a mutual recognition agreement on cybersecurity," while reaffirming that US conformity assessment bodies can be designated as Notified Bodies under the EU Radio Equipment Directive for all essential requirements, including cybersecurity, a signal that the adequacy-style model this paper advocates is already being pursued at the highest political level.

9. A role for the OECD?

We inhabit a sovereign world where multilateral organizations have fewer resources and at times lower levels (or uncertain levels) of commitment. Voluntary commitments to overseas development by states have dropped by billions of dollars in 2025 due to falling contributions by member states.[56] The United States has paused funding to numerous international bodies and withdrawn from a group of bodies.[57] Yet amidst this broader context the OECD is uniquely positioned to play a key role in fostering greater international alignment. With its convening power, analytical expertise, and multistakeholder reach, it can drive meaningful regulatory coherence:

Convening a regulatory hub: The OECD is uniquely positioned to act as an international hub for cybersecurity regulators. It can establish a regular forum (through its Digital Security Working Party) where national regulators and policymakers meet periodically to compare approaches, share best practices, and coordinate implementation of cyber rules. By providing a neutral platform that includes most major economies, the OECD can streamline currently siloed efforts and foster a community of practice among regulators.

Evidence-based policymaking: With its analytical expertise, the OECD can measure and highlight the impact of fragmented regulations. For example, it could research the economic and security costs of inconsistent incident reporting timelines or multi-factor authentication rules across countries. Such evidence-based reports could help build the case for alignment by quantifying how divergence undermines cybersecurity (e.g. diverting resources to compliance). The OECD's impartial data and recommendations can guide governments toward informed alignment efforts without singling out any one country's model.

Developing common standards & reciprocity: The OECD can facilitate the creation of common baselines and mutual recognition agreements (MRAs). Through its policy

[55] Ibid and see Baker McKenzie. (2025, August 25). EU and US announce framework trade agreement. *Global Sanctions and Export Controls Blog*. https://sanctionsnews.bakermckenzie.com/eu-and-us-announce-framework-trade-agreement/

[56] Hamann, S. (2026). Foreign Aid at a Crossroads: How Funding Cuts Reshape Global Development Cooperation. *Global Policy*, *17*(1), 122-133.

[57] Cogan, J. K. (2025). The Trump Administration Signals Major Reevaluation of US Engagement with International Organizations. *American Journal of International Law*, *119*(4), 777-789.

committees, it could draft model guidelines or principles for key areas (like incident notification thresholds, timelines, or baseline security controls) that members could adopt domestically. It can also encourage bilateral or multilateral **reciprocity agreements**– where countries agree to recognize each other's cybersecurity regulations or certifications, reducing duplicate compliance. Leveraging OECD's standard-setting experience ensures any alignment framework is vetted internationally and voluntary, easing acceptance by sovereign states.

In that regard, during the Sciences Po and LSE event, the Korea Internet & Security Agency (KISA), offered to share MRA structure between Korea and Singapore within an OECD forum to serve as a model for future work involving other countries.

Multistakeholder engagement: Advancing alignment requires input beyond governments alone. The OECD can integrate perspectives from industry (via BIAC), academia, and civil society by forming a **multistakeholder working group or expert panel** under its auspices. This group could regularly meet to identify pain points in regulatory divergence and propose solutions (e.g. mapping overlapping requirements or suggesting updates to outdated rules). By including non-governmental experts, the OECD would ensure that alignment efforts address real-world operational challenges and that proposed solutions enjoy broad support. BIAC, for instance, can supply technical expertise and private-sector viewpoints to inform OECD recommendations.

Global leadership and expansion: The OECD can serve as a **global champion for regulatory coherence**. Its work can set benchmarks that promote coordination in other international forums (e.g., G7) and guide countries outside the OECD to consider improved alignment.

Furthermore, the OECD is perceived as being an economic rather than security actor – enabling it to approach cybersecurity through a neutral economic and social lens. This neutrality is especially important against the context of renewed geopolitical tensions and live wars in 2026.

The economic lens the OECD brings is also relevant given sluggish growth and growing caution about binding international regulatory agreements. The OECD is both functional and consensus-driven and does useful work on standards. Beside technical standardization organizations, the Paris-based institution has served as the primary international standard setter in digital security since 1990, developing recommendations that support stakeholders in crafting policies aligned with economic prosperity, such as the 2022 Policy Framework on Digital Security.[58]

The OECD is also an adept convener. It has long worked with multiple stakeholders including business and technical experts. This multistakeholder approach has consistently delivered results. The OECD's 2022 Recommendation on Digital Security Risk Management, adopted by Council, developed useful principles even if non-binding ones.[59] The OECD has proven flexible in shaping agendas and including different

[58] OECD (2022), *OECD Policy Framework on Digital Security*, OECD Publishing, Paris
[59] Craig, A. J. (2023). Cyber security. In *The Elgar Companion to the OECD* (pp. 266-278). Edward Elgar Publishing.

participants. It maintains an ambitious agenda by publishing consensus-building research and gathering a wide community of public and private experts. While states remain in the driving seat, the organization manages to move beyond the polarization that paralyzes many other international institutions.

> *Regulatory cooperation mechanisms matter profoundly for economic growth and national security.*

Regulatory cooperation mechanisms matter profoundly for economic growth and national security. Research demonstrates that transparency mechanisms and mutual recognition provisions generate significant positive trade effects by reducing duplicative conformity assessments.[60] Harmonization and mutual recognition create level playing fields, are more efficient and can reduce errors. The OECD has documented these extensively, evidencing how regulatory cooperation reduces costs while maintaining protective standards. OECD research finds that transparency mechanisms and mutual recognition of TBT conformity assessment procedures have "significant, positive and rather strong trade effects," partly because they represent the simplest first step toward regulatory coordination.[61]

A 2016 OECD working paper on mutual recognition agreements is one of the most powerful examples of how mutual recognition agreements deliver value.[62] It found that when properly designed with appropriate preconditions and success factors, mutual recognition agreements deliver meaningful benefits by preventing duplicative testing and certification requirements.[63]

The OECD's core mission of promoting policies for highest sustainable economic growth, employment, and rising living standards in member countries retains broad support across its membership and beyond. There is strong support from OECD member states for this work, including appetite to engage on regulatory alignment. In late 2024, multiple OECD member states– including the UK, Netherlands, Estonia, and Switzerland – openly backed making regulatory alignment a priority in OECD meetings. Meanwhile in late 2025, just before the Paris gathering, the UK, US, Netherlands, France, Sweden, Belgium, and Japan all expressed formal support for making this issue a priority in the *OECD's Programme of Work*.

> *The value of broader multilateral, multistakeholder engagement on cybersecurity and regulation is there.*

The OECD remains uniquely open and receptive to private sector views and real-world experiences. Its work on principles and standards bears fruit, even in sectors with

---

[60] See Lejárraga, I., Shepherd, B., & van Tongeren, F. (2018). *Quantifying the effects of international regulatory co-operation mechanisms within preferential trade agreements* (OECD Trade Policy Working Paper No. TAD/TC/WP(2018)6/FINAL); Jang, Y. J. (2018). How do mutual recognition agreements influence trade? *Review of Development Economics*, *22*(3), 95–114.
[61] Lejárraga, I., Shepherd, B., & van Tongeren, F. (2018). *Quantifying the effects of international regulatory co-operation mechanisms within preferential trade agreements* (OECD Trade Policy Working Paper No. TAD/TC/WP (2018)6/FINAL)
[62] Ibid
[63] Ibid

staunch competition. This can be seen in OECD work on privacy guidelines, artificial intelligence principles, and digital security frameworks. Regulatory coherence, alignment and coordination at home is as much of a problem in many countries as cross-border regulatory policymaking. The value of broader multilateral, multistakeholder engagement on cybersecurity and regulation is there. This can be organised by international organisations or by non-government actors like universities who are also neutral parties.

2 Forming the future

This policy paper argues that there is real economic value – and potential to boost growth – through a greater focus on targeting cybersecurity regulation more effectively. A properly strategic approach at home and internationally puts three ingredients firmly on the table:

- Simplification, particularly through reducing the variation and complexities of cyber incident reporting. This can be done at the national level but also through bilateral, "minilateral" or multilateral agreements.

- Mutual recognition agreements acknowledging respective sovereignty, joint cybersecurity goals, and mutual economic interests.

- Strategic applied dialogue that brings together regulators, national officials, experts and industry.

Actionable recommendations to advance "defragment" cybersecurity regulations are the following:

- Identify convergence on incident reporting and mutual recognition agreements as the "low-hanging fruits" of cyber regulation harmonization.

- Establish a single database of incident reporting forms and existing mutual recognition agreements to make existing frameworks legible for cross-border organizations and to support standardization efforts.

- Join existing regional frameworks for cyber regulation convergence, especially for countries with emerging cyber security legislation.

- Actively engage with fora such as the OECD Digital Security Working Party to design standard reporting forms and blueprints mutual recognition agreements.

- Launch an international sandbox initiative to test and evaluate new standards, with cross-border organizations reporting actual or simulated incidents and national authorities engaging in joint data treatment and investigation.

- Create an annual conference dedicated to cyber regulation convergence, modelled after the LSE-Sciences Po workshop in Paris in November 2025 and the September 2024 LSE-Wilton Park conference, to gather policymakers, public agencies, private experts, and academia in a neutral space where they can safely discuss current cybersecurity fragmentation and harmonization under Chatham Rules. The OECD is particularly well placed to steward such dialogues, which should be opened to all countries, especially the ones driving regional frameworks.

lse.ac.uk/spp

School of Public Policy
The London School Economics
and Political Science
Houghton Street
London WC2A 2AE

Email: spp@lse.ac.uk