

BUSINESS at OECD | Business and Industry Advisory Committee to the OECD

Resolving Cybersecurity Regulatory Fragmentation for Security and Economic Growth

Business Evidence to Strengthen Cyber Resilience

Policy Paper
November 2026

Contents

Executive Summary 3
Introduction 5
Findings from the *Business at OECD* Survey 7
Economic Costs of the Status Quo 7
Direct costs 7
Indirect costs 7
Impact of Fragmentation 9
1. Incident reporting and notification 9
2. Supply-chain and third-party requirements 9
3. Data protection and security operations 10
4. Conflicting requirements: sector-specific and vertical overlaps 10
The Effect of Fragmentation on Cybersecurity Outcomes 14
Taking Actions: A Path Toward Regulatory Coherence 16
Practical Priorities for Policymakers 17
Mobilising the OECD 19
Build the evidence base 19
Convene stakeholders 19
Develop practical guidance 19
Conclusion 20
Business at OECD (BIAC) National Members 22

© 2026 *Business at OECD* (BIAC). All rights reserved. No part of this publication may be reproduced or transmitted in any form or by any means, including photocopying and recording, or by any information storage and retrieval system.

Executive Summary

Cyber threats are escalating in scale, sophistication and economic impact, with the global cost of cybercrime projected to reach EUR 14 trillion by 2029.[1] In response, governments across the OECD have expanded their cybersecurity laws, standards and regulatory frameworks, introducing new requirements to protect critical systems and digital economies. While well-intentioned, these measures have resulted in increasing regulatory fragmentation, creating a complex and often inconsistent global landscape that imposes significant costs on businesses and undermines effective cyber defence.

Fragmentation is not only an economic issue but is also a risk for national security. Divergent regulatory requirements prevent organisations from implementing centralised and optimised cybersecurity systems, fragmenting expertise and reducing economies of scale. Restrictions such as data localisation and inconsistent reporting frameworks can create operational silos, limiting threat intelligence sharing and weakening situational awareness.

In April 2025, Chief Information Security Officers (CISO) from companies across sectors issued a letter[2] to G7 countries and OECD Member States. It warned that increasing regulatory divergence across different jurisdictions limits the ability of governments and private sector entities to share intelligence efficiently, weakening collective cyber resilience.

At the request of its members, *Business at OECD* (BIAC) has worked to document the costs businesses face due to cybersecurity regulatory fragmentation and the related risks posed to our shared digital security environment.

In this context, in November 2025, *Business at OECD* supported a joint conference organised by Sciences Po and the London School of Economics with support from Microsoft, which convened business, civil society, government, academia, and the OECD to address cybersecurity regulatory fragmentation. The resulting conference report, *Defragmenting International Cyber Security Regulations*,[3] underlines the negative impacts on resources for cyber defence, investor confidence and economic growth.

Contributing to this objective, in January 2026 *Business at OECD* surveyed its members to gather business evidence on cybersecurity regulatory fragmentation. Twenty-five multinational enterprises across sectors, with operations in Asia, Europe, Oceania, Africa and the Americas, responded, providing over 1,200 data points, both quantitative and qualitative.

Evidence from the *Business at OECD* survey highlights that cybersecurity regulatory fragmentation and related compliance obligations divert critical resources away from operational security and cyber defence; in some cases, localised solutions have also created operational risks and vulnerabilities. In turn, this impacts investor confidence, impeding economic growth, cross-border trade and investment.

Firms operating across multiple jurisdictions face overlapping requirements that generate recurring burdens. More than one third of surveyed organisations report annual costs exceeding EUR 1 million to manage fragmentation. Beyond direct financial impacts, fragmentation slows innovation, delays market entry and discourages investment, particularly where compliance costs outweigh commercial opportunities.

The *Business at OECD* survey on cybersecurity regulatory fragmentation identified four areas where fragmentation is most acute and damaging:

- **Incident reporting**, where divergent timelines, thresholds and formats impose significant operational strain during the critical response period;

- **Supply-chain compliance**, characterised by cascading requirements across partners;
- **Data governance and localisation**, which constrain global security operations and advanced threat detection capabilities;
- **Conflicting requirements** between overlapping sector-specific and vertical regulations, creating inconsistent obligations across jurisdictions and industries.

Incident reporting is where the operational burden is sharpest and where action is most needed. Behind all four areas lie broader structural drivers: geopolitical tensions, acute cybersecurity skills shortages, and technologies, with AI at the forefront, evolving faster than regulatory frameworks can track. Together, they contribute to a patchwork of rules that increases complexity while failing to deliver proportional security benefits.

Business stakeholders emphasise that coordinated international action on greater coherence and interoperability can strengthen security outcomes and reduce unnecessary costs. Priority areas for progress include:

- Streamlining and aligning incident reporting requirements;
- Adopting risk-based regulatory approaches;
- Enabling mutual recognition of certifications;
- Strengthening capacity-building efforts to address these skills gaps;
- Early and structured business engagement in advancing cybersecurity regulatory cooperation.

Importantly, *Business at OECD* calls on the OECD through its Working Party on Digital Security to serve as a forum for collecting data, fostering dialogue and evidence-based analysis to provide clarity and solutions for concrete action towards reducing cybersecurity regulatory fragmentation, including incident reporting as an immediate and actionable issue.

The OECD is uniquely positioned to lead this effort. As a trusted platform for structured multistakeholder dialogue, the Organisation can help map where fragmentation costs the most and where common ground already exists and identify how to promote both convergence (the substantial alignment of legal requirements) and interoperability (the ability of different regulatory systems to operate together) across cybersecurity regimes. A dedicated OECD recommendation would give governments concrete, actionable guidance for pursuing cybersecurity regulatory coherence, effectively bringing jurisdictions and relevant stakeholders together for meaningful dialogue.

This report highlights key conclusions from a *Business at OECD* survey, related desk research and input from national business federations. It presents private sector initiatives to address and mitigate cybersecurity risks, proposes proactive solutions towards reducing regulatory fragmentation in this domain, and shares significant costs imposed by fragmentation resulting from well-intentioned government regulations.

Collaboration between international organisations, governments, and industry is essential to translating these efforts into impactful, real-world solutions. This report aims to help advance this important and shared objective.

Introduction

The annual cost of cybercrime worldwide is projected to reach EUR 14 trillion by 2029.[4] Malicious cyber threats continue to target companies, governments and society, with significant financial implications and a loss of trust. The average cost of a single data breach rose by 10% between 2023 and 2025, to USD 4.88 million. The associated business losses rose by nearly 11% in the same period.[5] Fragmentation can increase the risk of cybercrime and complicate businesses' ability to defend against threats.[6]

The growing use of artificial intelligence threatens to further amplify the frequency and risks of cyberattacks. This is part of a broader change in the nature of cyberattacks – harder to predict and with AI-boosted capabilities. There is also a persistent evidence gap on AI misuse in cyberspace, further hindering informed policymaking in a rapidly changing environment. At the same time, advances in quantum computing create a longer-term risk to widely-used cryptographic methods and reinforce the need for coordinated migration to post-quantum cryptography.

In response to growing cyber threats, several governments have responded by expanding their cybersecurity laws, standards and regulatory frameworks, with specific attention to critical systems protection, treating cybersecurity as a national security priority. However, this has also led to increased divergence, a consequence of overlapping and duplicative rules across countries and sectors.

At the same time, cybersecurity remains an area where many regulators have limited expertise, often siloed within domestic teams and where regular international exchange with peers is lacking. The result of this fragmentation is a diversion of resources from operational cyber defence to compliance, raising both cost and risk. It also results in less effective systems and deteriorated threat detection processes, directly and indirectly inhibiting optimal cybersecurity practices.

The growing divergence amongst domestic efforts across sectors is coupled with increasing restrictions on digital innovation and investment, and impediments to trusted cross-border data flows. Even instruments designed to make data governance regimes interoperable, such as bilateral and plurilateral digital agreements, can create a "patchwork of rules" that further complicates efforts to address cybersecurity.[7]

Emerging technologies threaten to further amplify the frequency and risks of cyber-attacks.

Cybersecurity regulatory fragmentation is a shared challenge for governments and industry across sectors. The OECD, and particularly its Working Party on Digital Security, is well positioned to serve as a forum for developing the evidence base needed to better understand and measure these issues, and to facilitate the dialogue and analysis necessary to advance meaningful solutions to this growing challenge.

Considering the costs and risks, as well as impacts on investor confidence, Business is raising awareness around this important issue. In April 2025, Chief Information Security Officers (CISOs) from companies globally across sectors issued a letter[8] to G7 and OECD Member States, highlighting key challenges in the cybersecurity regulatory landscape and how increasing divergence between regulatory frameworks limits the ability of stakeholders to share intelligence efficiently, weakening collective cyber resilience.

In follow-up to the CISOs letter, at the request of its members, *Business at OECD* (BIAC) launched an initiative documenting the related costs businesses are facing, while advocating for greater cooperation to address the risks posed to our shared digital security environment.

Recent initiatives are also reaching similar conclusions. In March 2026, the Cybersecurity Tech Accord, a global alliance of more than 150 technology companies, issued a statement on Advancing International Alignment in Cybersecurity Regulation to Strengthen Collective Resilience, including five recommendations to governments. [9]

Furthermore, the recent OECD report "Towards international coherence of cybersecurity regulations", provides an overview of the growing fragmentation of cybersecurity regulations across jurisdictions, and outlines consequences for both governments and businesses.

This *Business at OECD* report therefore shares key insights from a survey of companies on their experience of cybersecurity regulatory fragmentation, complemented by desk research and input from national business federations. Through this overview, we highlight costs of cybersecurity regulatory fragmentation for businesses across sectors and propose avenues of future work that could meaningfully contribute to reducing the compliance burdens, cost and risk that uncoordinated regulatory systems impose on our collective cybersecurity.

Findings from the *Business at OECD* Survey

In January 2026, *Business at OECD* launched a survey of its members to gather business evidence on the landscape of cybersecurity regulatory fragmentation. We received responses from 25 multinational enterprises across sectors, with operations in Asia, Europe, Oceania, Africa and the Americas, including over 1,200 data points.

Evidence from the *Business at OECD* survey underlines that fragmentation diverts critical resources away from operational security towards compliance activities. A number of significant challenges have been driving cyber regulatory fragmentation, including growing geopolitical mistrust, which limits intelligence sharing and mutual recognition of another jurisdiction's assessments, certifications, or assurance mechanisms.[10] At the same time, concerns over "digital sovereignty" reflect a desire on the part of governments for full control over infrastructure, data and incident information, while they diverge regarding cybersecurity models, choosing between following a more state-driven, market-driven, or rights-based approach. Finally, skills shortages leave governments and businesses, in particular small and medium-sized enterprises (SMEs), short of cybersecurity expertise. As a result, organisations face slower response times and weakened situational awareness, while operational strain across cybersecurity functions, and the related costs, continues to rise.

Economic Costs of the Status Quo

Firms operating across multiple jurisdictions report that overlapping and inconsistent requirements translate into sustained and recurring compliance costs rather than one-off adaptation expenses. Fragmented cybersecurity rules also slow innovation, affect investment decisions, and impede cross-border digital activity. Duplicative compliance efforts divert funding from research, development and investment.

Direct costs

More than one third of surveyed organisations estimate that the cost of managing regulatory fragmentation exceeds EUR 1 million annually across their operations. These costs include legal analysis, duplicated audits and certifications, region-specific infrastructure investments, and the diversion of security and engineering resources to compliance activities. 92% of respondents indicated that reduced compliance costs would be a direct operational improvement from reduced regulatory fragmentation.

Individual cybersecurity certifications regularly exceed EUR 100,000 each, with cumulative costs reaching far higher when similar requirements must be satisfied repeatedly across jurisdictions. Data localisation alone can cost approximately USD 500,000 per country, plus around USD 50,000 per digital offer to maintain; a single compliance report can cost between USD 75,000 and 350,000 depending on the vendor.[11]

In addition, a *Request for Information on Cybersecurity Regulatory Harmonization* by the United States concluded that the lack of harmonisation and reciprocity is harming cybersecurity outcomes while increasing compliance costs through additional administrative burdens, noting that compliance spending drew resources from cybersecurity programs.[12]

Indirect costs

Direct financial costs represent only part of the burden. Respondents widely reported indirect costs that are harder to quantify but equally material. These include delayed product launches, postponed market entry, reduced scalability of security solutions and forgone innovation opportunities.

20% of firms indicated that fragmented requirements influence the sequencing and timing of market entry, with jurisdictions aligned to international standards being prioritised over those with highly bespoke regimes. Importantly, disproportionate regulatory obligations can delay or discourage entry where compliance costs outweigh market opportunities.

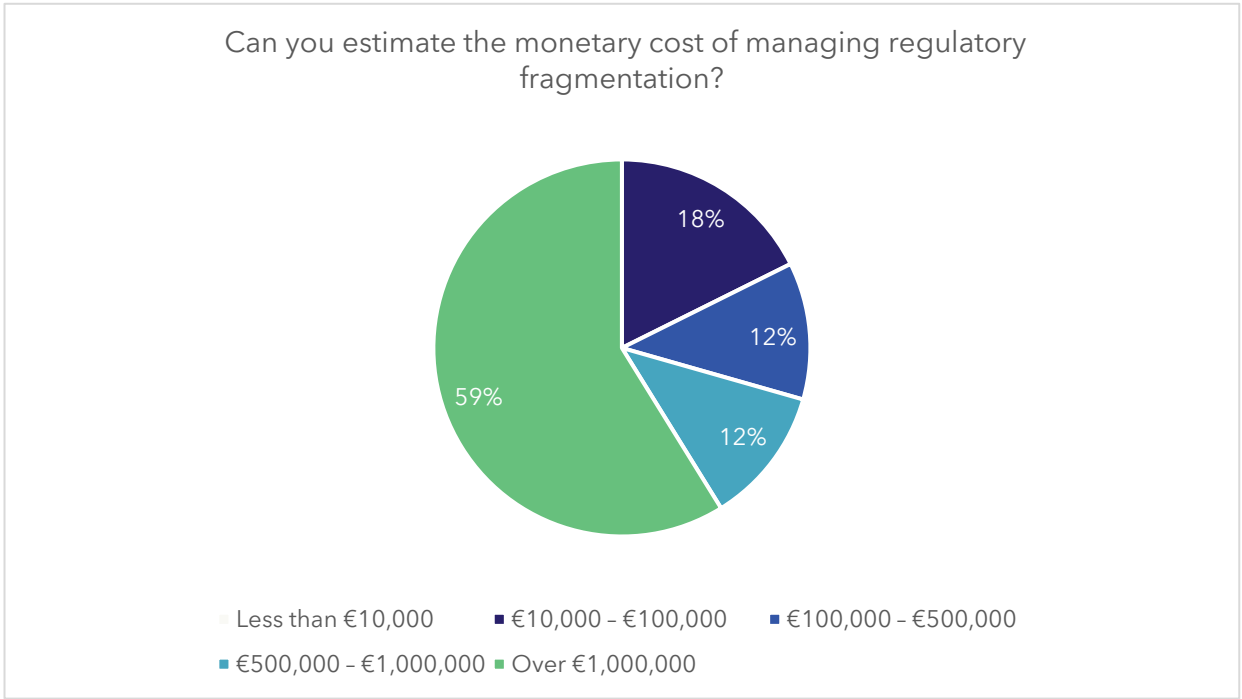
Entry into new markets may require the reworking of technical solutions to meet standards that diverge in small but impactful ways. The cost and time of adhering to local standards is a material driver of prioritisation of markets, and even large markets may experience delayed introduction of innovative products due to the burden of implementing nonstandard requirements.

An observation from the US communications sector underlines that, when "companies are required to divert resources from their cybersecurity programs to 'check the box' for an array of divergent cybersecurity regulations and requirements across jurisdictions," consumers are left "with unclear expectations about company cybersecurity practices." By contrast, a tiered structure allows "businesses to undertake their own risk and investment analyses based on each entity's unique considerations."[13]

Divergence between major jurisdictions also create competitive imbalances, particularly in fast-moving sectors, as is most notable between the European Union (EU) and the United States. The EU AI Act establishes a binding, risk-based regime with extensive obligations for providers and users of AI systems, including requirements on risk management, transparency and governance.

By contrast, the US has traditionally pursued a largely non-binding regulatory approach, relying on voluntary frameworks and sectoral initiatives rather than a comprehensive federal law. Such asymmetry leads to structural competitive effects, as European operators face higher compliance costs and regulatory constraints, potentially slowing time-to-market and innovation cycles.

Fragmentation also carries a security cost. Cybersecurity professionals assigned to duplicative compliance reporting are unavailable to defend networks or improve resilience. Nearly three-quarters of surveyed firms expect that reduced fragmentation would free up resources for direct cybersecurity operations. In a field already facing acute skills shortages, this opportunity cost applies to organisations of every size and sector.



Impact of Fragmentation

Survey responses make clear that while regulatory fragmentation is pervasive, its operational and security impacts are felt most strongly in a small number of areas. Firms consistently pointed to four key areas where fragmentation is the costliest, most complex and most damaging to effective cyber defence: incident reporting, supply-chain compliance, data localisation and overlapping sector-specific regimes.

1. Incident reporting and notification

Incident reporting obligations are identified by surveyed firms as one of the most acute sources of regulatory fragmentation requiring immediate attention. Sources of divergence include differing thresholds, obligations, timelines, portals and definitions, as well as a lack of coordination among authorities. 84% of respondents report that notifying authorities following a cybersecurity incident is a major compliance challenge, and 64% cite fragmented incident reporting obligations as a primary driver of operational complexity.

Firms emphasised that a single cyber incident frequently triggers multiple parallel reporting obligations across jurisdictions and regulatory regimes. Reporting timelines can range from as little as one hour to as much as 72 hours, depending on the applicable framework and national implementation.

Parallel reporting requirements divert scarce security, legal, and engineering resources at precisely the moment they are most needed for investigation, containment, and recovery. Several respondents reported that senior engineers and incident responders are routinely redirected from active defence to administrative filing tasks in the early stages of incident response.

The first hours after a significant incident are decisive for containment and recovery, and reporting obligations should be designed to support incident response. A "report once, use many" principle would allow one standardised notification, submitted through a single channel, to meet the needs of every competent authority.

2. Supply-chain and third-party requirements

Supply-chain and third-party requirements represent another area where fragmentation is felt particularly strongly. 92% of respondents identify supply-chain compliance as a significant challenge linked to regulatory fragmentation, making it the highest-ranked source of operational difficulty among the categories assessed.

Respondents described cascading obligations flowing from regulators to primary entities and then onward to suppliers, service providers, and subcontractors across jurisdictions. These cascading requirements frequently involve repeated audits, overlapping certifications, and duplicative documentation requests. This includes cases when identifying third-tier suppliers requires multiple tiers of approval. Firms also noted that evidence must often be provided multiple times to regulators, customers, and partners using different formats and assessment criteria.

These burdens can be especially acute for SMEs and for providers of critical services embedded in complex supply chains. SMEs often lack the resources to respond efficiently to repeated assessments, while critical service providers face heightened sector-specific scrutiny from multiple authorities simultaneously. As such, fragmentation risks raising barriers to participation in regulated supply chains and thereby reducing supplier diversity.

3. Data protection and security operations

Inconsistent data rules and data localisation requirements were widely cited as constraining effective cybersecurity operations. Respondents explained that data localisation and transfer restrictions frequently prohibit the aggregation of security telemetry across borders, limiting centralised monitoring, analytics, and threat intelligence correlation. Where data cannot leave a jurisdiction, security teams lose sight of activity across their wider systems, and the resulting blind spots reduce actual security effectiveness. 28% of respondents noted that operational risks and vulnerabilities were created by localised solutions.

These constraints can reduce firms' ability to deploy global security operations and to leverage advanced, AI-driven threat detection capabilities that depend on large, diverse data sets. Several respondents reported that security architectures must be segmented by jurisdiction to comply with local rules, even where this undermines consistency and increases operational complexity.

There is a growing misalignment between cybersecurity objectives and data governance frameworks. Cybersecurity outcomes depend on timely access to comprehensive operational data; however, localisation requirements often prioritise data residence over security effectiveness, a risk that applies to every sector holding sensitive or operational data. Respondents stressed that this tension weakens collective defence and complicates cross-border incident response, particularly for attacks that propagate across regions.

4. Conflicting requirements: sector-specific and vertical overlaps

Highly regulated firms face acute challenges from overlapping and often inconsistent obligations imposed by horizontal cybersecurity frameworks and sector-specific or product-specific regimes. Respondents in finance, telecommunications, transport, travel and tourism, healthcare and industrial sectors reported that parallel requirements apply to the same underlying systems and incidents, often without clear prioritisation or coordination.

These overlaps undermine centrally steered Information Security Management and global security governance models. Firms explained that controls must be adapted or duplicated to satisfy divergent sectoral rules, reducing efficiency and increasing the risk of inconsistency across the organisation.

For example, at present, one security control must often be documented and proven multiple times for multiple authorities, resulting in what has been referred to as *security debt*.

National divergences further exacerbate the problem. Respondents in the European Union highlighted that national transpositions of common legislation can result in distinct registration requirements, incident thresholds, reporting channels, and supervisory practices. Delayed and uneven transposition compounds this divergence. As of mid-2026, several EU Member States have yet to complete transposition, leaving firms to operate under provisional or overlapping national regimes.

Sector-specific or technology-specific cybersecurity regulations can also overlap with horizontal frameworks, creating challenges for operators in these spaces. This undermines the benefits of regulatory coherence, forcing firms to manage compliance on a country-by-country basis, even within integrated markets. Clarifying the scope and interaction between regulations would enhance legal certainty, avoid duplication and ensure consistent application across the EU.

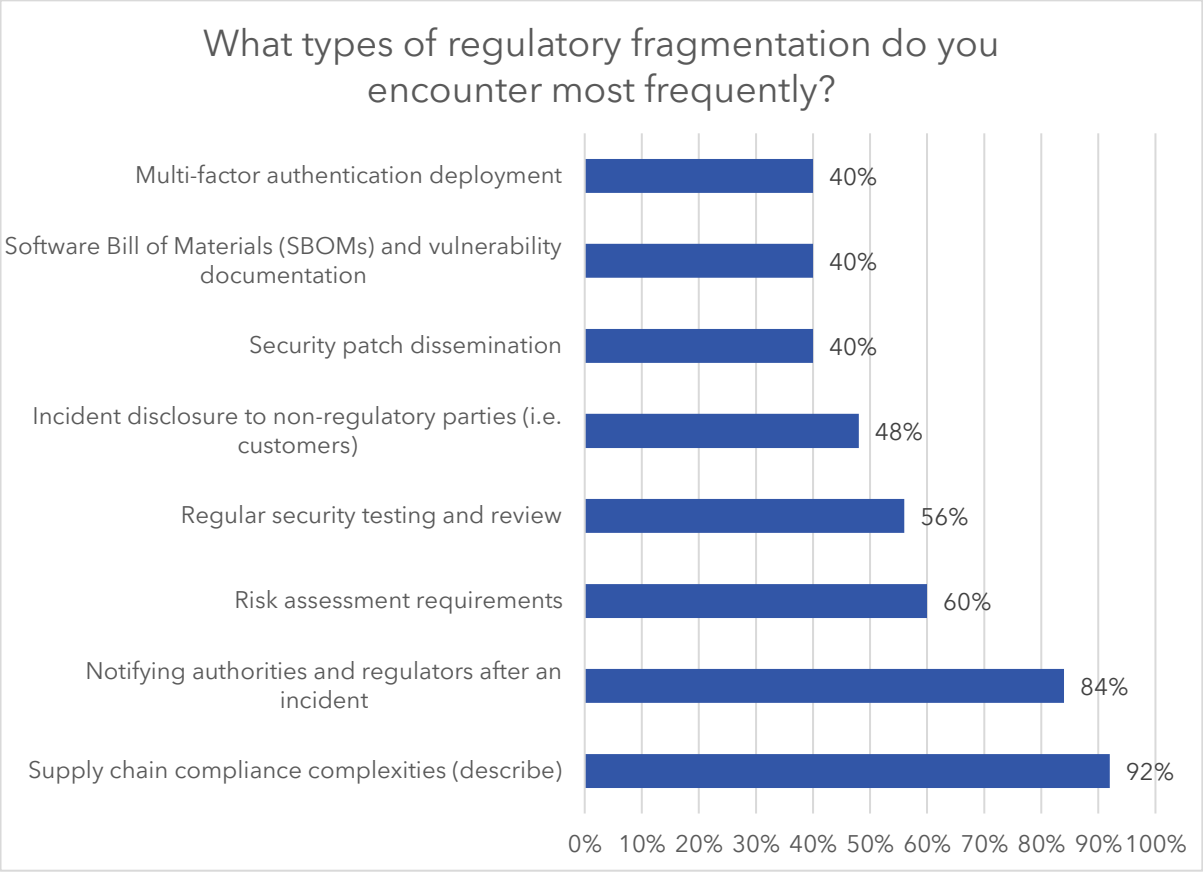
There is room for improvement – particularly on reporting timelines and classification of notifiable incidents. In Australia, the Security of Critical Infrastructure (SOCI) Act distinguishes between critical incidents with a significant impact on an asset, reportable

within 12 hours, and those with a lesser but relevant impact, reportable within 72 hours. Harmonising reporting timelines between and within classifications would reduce the administrative burden for companies operating both in Australia and beyond.

Sector-specific rules are not necessarily problematic when tailored and limited to the areas where they are strictly necessary. Seen on their own, most requirements and standards are thoughtfully designed and align with universal cybersecurity principles.

The difficulty appears when requirements are viewed from the perspective of a global company, as many authorities add their own national specificities to common standards, and the sum of these adaptations is fragmentation.

For example, a telecoms operator offering cloud-based services across multiple jurisdictions must navigate national data localisation laws, sector-specific cybersecurity mandates, and international privacy regulations simultaneously.[14] This patchwork of regulations increases operational costs and forces operators to implement duplicative or overly cautious security measures, discouraging innovation and investment in new technologies.



Box. Examples of Recent National and Regional Developments

Australia: Australia's primary cyber incident reporting requirements for critical infrastructure are set out in the Security of Critical Infrastructure (SOCI) Act. Responsible entities must report incidents to the Australian Cyber Security Centre within 12 hours if they have a significant impact on the availability of a critical infrastructure asset, and within 72 hours if the impact is considered relevant but less severe. The scope of reportable incidents remains broad under the Act's all-hazards approach, creating uncertainty about whether non-malicious events, such as technical outages or engineering failures, may also be covered. Recent reforms, including the Cyber Security Act 2024, further strengthen Australia's cyber resilience framework by introducing a 72-hour reporting requirement for ransomware and cyber extortion payments. Together, these measures aim to improve cyber threat visibility, information sharing, and coordinated responses to significant incidents while strengthening national cyber resilience and preparedness.

Canada: Canada is implementing the Critical Cyber Systems Protection Act (CCSPA) to strengthen cybersecurity and resilience across critical infrastructure sectors. The Act requires mandatory cybersecurity programs and cyber incident reporting, and aims to improve visibility of threats, information sharing and regulatory coordination across sectors. Canada has established incident reporting as a core element of the CCSPA framework, there is no fixed reporting timeline equivalent to the EU's 24-hour/72-hour reporting model or the timelines contemplated under the US framework. Instead, the government has indicated that reporting requirements and related processes will be developed through the Act's regulatory implementation process, while specifying that the prescribed reporting period may not exceed 72 hours.

European Union: The EU has established one of the most comprehensive and structured cyber incident reporting frameworks through the Network and Information Systems (NIS2) Directive and the Cyber Resilience Act (CRA). Under NIS2, entities are required to report significant incidents using a phased approach that includes a 24-hours early warning, a 72-hours incident notification, and a final report within one month. Reporting obligations are triggered by significant incidents that cause, or are capable of causing, severe operational disruption, significant financial loss, or material harm to other organisations or individuals. The CRA introduces similar incident and vulnerability reporting obligations for products with digital elements, including incident reporting timelines that largely mirror the NIS2 framework. However, for actively exploited vulnerabilities, the CRA requires a final report within 14 days of implementing a mitigating or corrective measure. At the same time, the CRA uses a distinct definition of a reportable incident despite incorporating NIS2's baseline definition of an incident by reference. This illustrates how interoperability challenges can arise even within a single jurisdiction, where two overlapping instruments define a reportable incident differently.

The European Commission's Digital Omnibus package (November 2025) proposes a single entry point for incident reporting, managed by ENISA, allowing one notification to satisfy obligations under the NIS2 Directive, the GDPR, DORA, eIDAS and the CER Directive on a "report once, share many" basis. It is complemented by the common incident-reporting templates adopted by the NIS2 Cooperation Group in May 2026. Neither measure, however, changes the underlying legal requirements, such as divergent timelines, thresholds and information requirements; a common portal is a necessary but not sufficient condition.

United States: The US's Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) directs the Cybersecurity and Infrastructure Security Agency (CISA) to establish mandatory cyber incident reporting requirements for covered critical infrastructure entities. CIRCIA defines a cyber incident as an occurrence that actually jeopardises, without lawful authority, the integrity, confidentiality, or availability of information on an information system, or jeopardises, without lawful authority, an information system. A cyber incident will be reportable as a "covered cyber incident" if it satisfies substantiality criteria established in the final rule, set to be published later in 2026. Under the statute, covered entities will be required to report covered cyber incidents within 72 hours and ransomware payments within 24 hours. CIRCIA also establishes the Cyber Incident Reporting Council to help coordinate and harmonise federal cyber incident reporting requirements across agencies. While the law has been enacted, the reporting regime has not yet been implemented and will not take effect until CISA completes the rulemaking process and publishes a final rule. The March 2026 Cyber Strategy for America underlines the importance of better aligning regulators and industry globally.

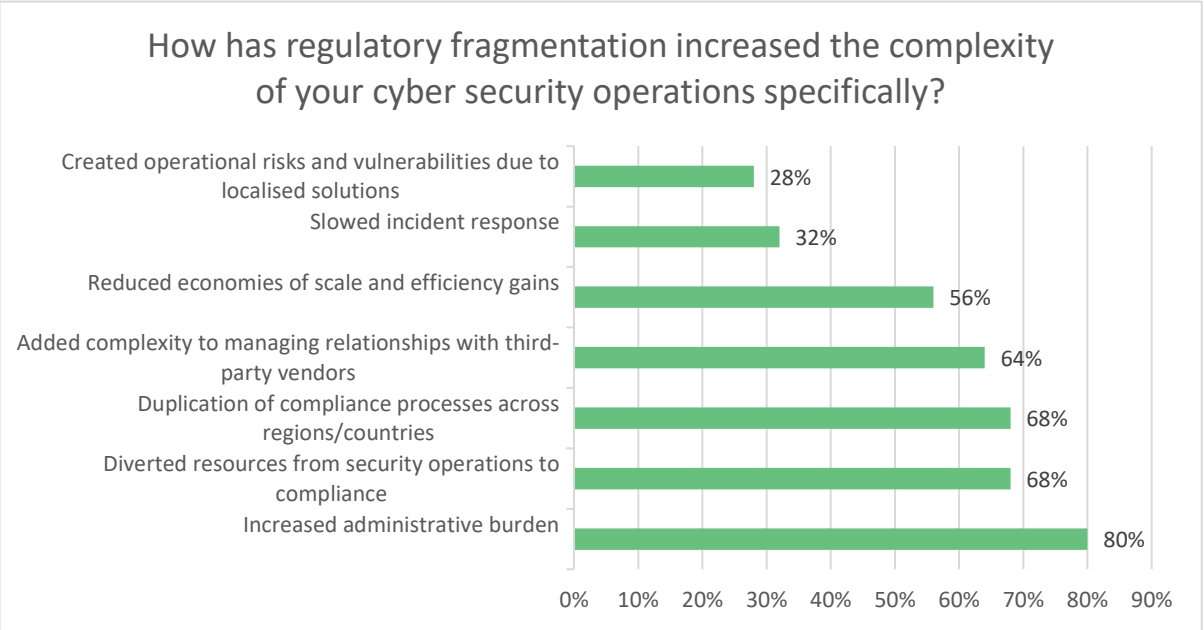
United Kingdom: The UK is modernising its cyber regulatory framework through the Cyber Security and Resilience Bill, which updates the existing Network and Information Systems (NIS) regime to strengthen cybersecurity and resilience across critical sectors. The proposed framework expands coverage to additional digital service providers, managed service providers, data centres, and certain critical suppliers, while enhancing incident reporting obligations and regulatory oversight. The Bill is also designed to promote greater consistency across sectors and regulators, recognising the importance of a coherent and effective cyber resilience framework. The Bill requires an initial notification within 24 hours and a fuller report within 72 hours, but no final report after one month as specified under NIS2. However, the Bill creates some overlapping reporting requirements and does not take the same streamlined approach that the EU is taking. Thresholds for incident reporting and other details are yet to be defined and will be set through secondary legislation over the coming year.

Japan: Japan's approach illustrates a different trend, choosing to create an entirely new mandatory reporting obligation to be applied on top of previously informal information-sharing processes. The Active Cyber Defense Act, enacted in May 2025, introduces for the first time a binding requirement for operators of critical systems across fifteen sectors, including energy, telecommunications, finance and healthcare, to report cybersecurity incidents to sectoral ministries and Japan's National Cybersecurity Office. The law is being phased in through 2026 and 2027, with core reporting obligations expected to take effect around October 2026, though the precise scope and timelines of what must be reported are still being finalised in secondary guidance.

New Zealand: New Zealand does not currently have a cyber incident reporting law that imposes uniform statutory reporting deadlines across critical infrastructure sectors. Instead, the National Cyber Security Centre (NCSC), part of the Government Communications Security Bureau (GCSB), operates a national cyber incident reporting framework under which organisations, government agencies, and critical infrastructure operators are encouraged or required under sector-specific obligations to report cybersecurity incidents to the NCSC. Government agencies are required to report all cybersecurity incidents to the NCSC, while the NCSC provides incident response services and reporting channels for organisations across New Zealand. The NCSC defines incidents of national significance as those affecting critical infrastructure or having the potential to impact large groups of New Zealanders and uses a severity-based categorisation framework, including "highly significant" incidents that impact sensitive data or disrupt essential services. The current focus remains on centralised incident reporting.

The Effect of Fragmentation on Cybersecurity Outcomes

Regulatory fragmentation in cybersecurity does more than impose significant costs on businesses, it increasingly undermines the security objectives the rules seek to achieve. By constraining coordination and dispersing resources, fragmentation weakens the ability of organisations to detect, respond to, and recover from cyber threats that are inherently cross-border.



Slowing incident response

A single incident can trigger multiple parallel notification requirements under different frameworks, each with distinct timelines, thresholds, formats, and submission channels. This puts further strain on security operations with senior security, legal and engineering staff being pulled away from remediation to produce documentation. 84% of firms note that notifying authorities and regulators after an incident is one of the most frequent sources of regulatory fragmentation experienced.

The cumulative security impact is tangible. Respondents associated fragmentation with slower deployment of patches and security tools, delayed incident response and uneven security postures across regions. Several explicitly warned that a compliance-driven approach risks prioritising checklists over risk reduction, resulting in higher effort but weaker overall resilience.

Nearly three-quarters of firms note that reduced regulatory fragmentation would result in greater resource availability for direct cybersecurity operations.

Hampering threat detection

It was consistently noted that fragmented rules impede centralised threat detection and situational awareness. Requirements for localised data storage, specific monitoring tools, or national reporting portals prevent security teams from correlating threat intelligence across regions and identifying emerging attack patterns at scale. These regional silos, several respondents emphasised, create blind spots that sophisticated attackers are capable of exploiting. 80% of firms indicated that they would experience improved cross-border cooperation if regulatory fragmentation were reduced.

Undermining centralised security management

Firms often need to localise security architectures and teams to meet jurisdiction-specific requirements. This prevents them from being able to rely on centralised, globally optimised security operations. Respondents stressed that this approach fragments expertise and reduces economies of scale, ultimately limiting the ability to deploy advanced security tools uniformly across the organisation.

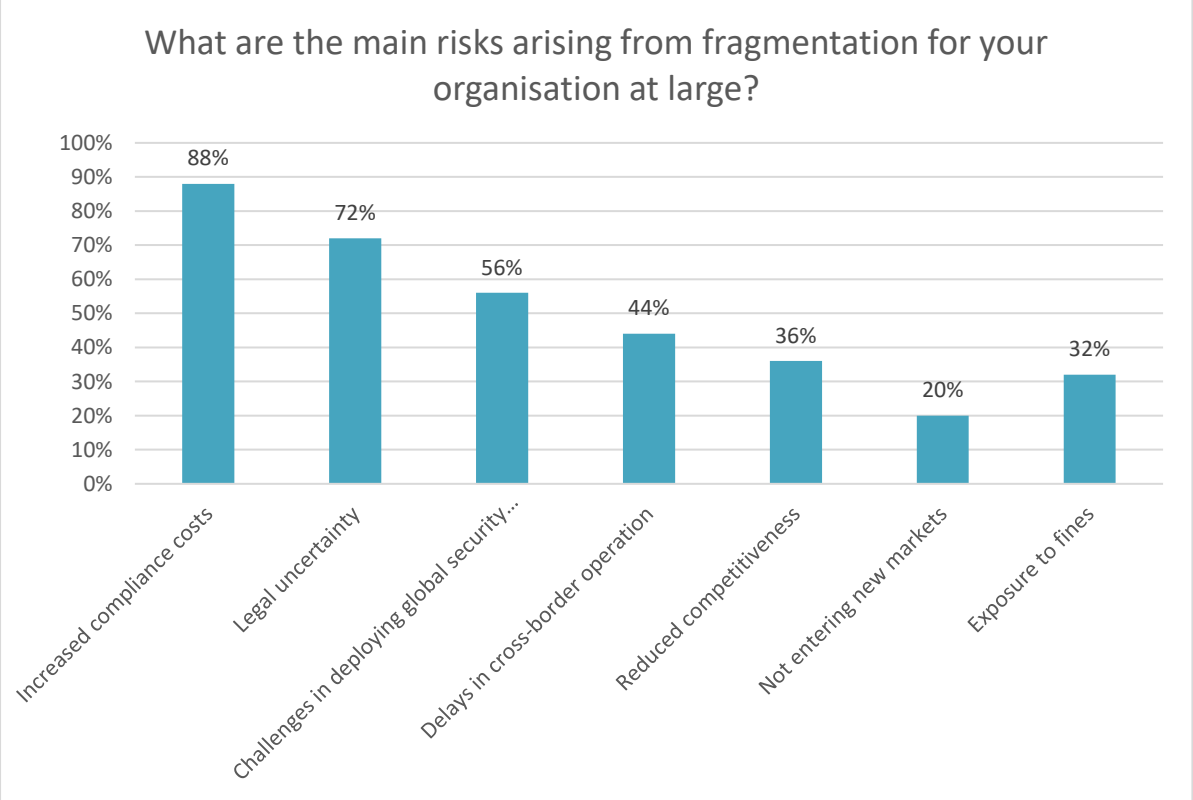
Crowding out through administrative burden

Differences in regulatory scope and implementation mean that compliance efforts often cannot be reused or scaled efficiently, even where policy goals are aligned in principle. 68% of respondents report experiencing the duplication of compliance processes across regions and countries, and 56% report experiencing reduced economies of scale and efficiency gains due to the increased complexity brought by regulatory fragmentation to cybersecurity operations specifically.

Firms must map, document, test and report a single framework in multiple formats to satisfy parallel regimes, which results in duplication that crowds out investment in proactive security capabilities in favour of compliance capacity. 68% of firms explicitly note that cybersecurity regulatory fragmentation has resulted in the diversion of resources from security operations to compliance.

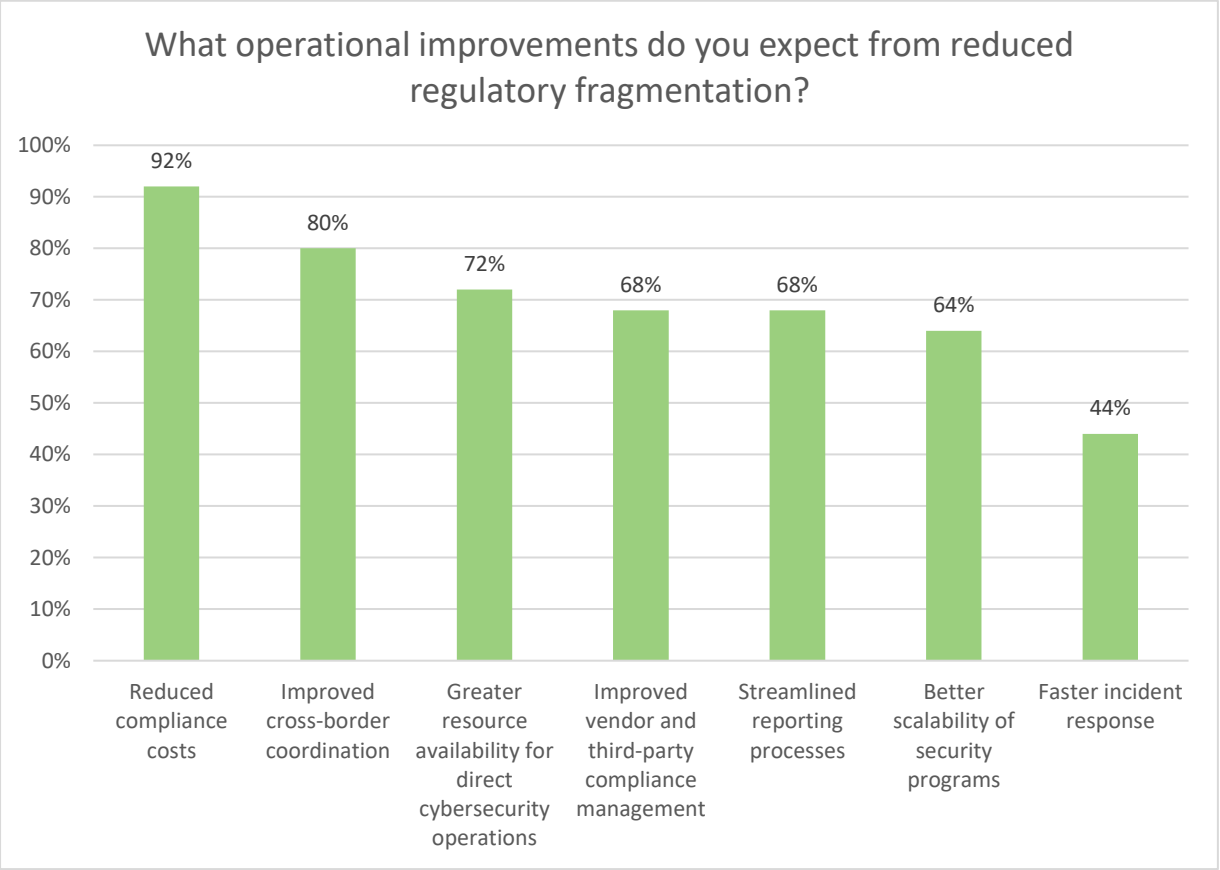
Exacerbating labour market constraints

These pressures are magnified by labour market constraints. Firms repeatedly underscored the scarcity of professionals who possess combined cybersecurity, legal, and regulatory expertise. Fragmentation increases demand for these hybrid profiles while forcing existing security engineers to devote substantial time to documentation, reporting, and audit preparation. Respondents warned that this shift from operational defence to administrative compliance exacerbates burnout and talent retention challenges across already constrained teams and discourages long-term investment in cybersecurity skills.



Taking Actions: A Path Toward Regulatory Coherence

Urgent action by policymakers is needed. Businesses are already absorbing the costs and risks of cybersecurity regulatory fragmentation, and investment in parallel control frameworks and internal compliance mapping across regulatory regimes is yielding diminishing returns at escalating costs.



Enhanced cooperation among regulators and policymakers on cybersecurity regulatory coherence would reduce overlaps and compliance burden, supporting greater alignment and interoperability.

The fragmentation problem is relevant for business and governments alike and calls for collective action through international, multistakeholder coordination.

Business evidence demonstrates that fragmentation is eroding resilience, trust, investment and consumer confidence, and ultimately economic growth, without delivering proportionate security benefits. The actions presented in the next section merit the urgent attention of policymakers with the support of the OECD.

Practical Priorities for Policymakers

Greater international coherence is achievable through incremental multistakeholder policy dialogue focused on solutions that are both practical and interoperable. Drawing on its members' survey feedback, *Business at OECD* has identified five priority areas where cooperation would have the most impact: streamlining incident reporting, aligning on risk-based outcomes, reducing duplication through mutual recognition, improving capacity building, and structured business engagement. AI governance also deserves attention, since emerging AI requirements could exacerbate existing cybersecurity fragmentation. Aligning the reporting and response processes for AI security incidents with existing cybersecurity incident management, for example, would reduce duplication and promote regulatory coherence.

Through instruments such as the OECD Recommendation on Digital Security Risk Management, the OECD has developed multistakeholder guidance on the economic and social prosperity dimensions of digital security risk. It has also produced practical guidance on digital security governance, critical infrastructure protection, and cross-border data flows, and increasingly provides a venue for member states to exchange experiences on the implementation and effectiveness of domestic cybersecurity regulations. As cyber threats have intensified and governments have rapidly expanded their rules, this role as a platform for dialogue and convergence has become even more critical.

The priorities below were identified by *Business at OECD* for the attention of policymakers and the OECD's future work.

1. Streamline incident reporting

In the *Business at OECD* survey, 84% of companies identified incident reporting as a major source of fragmentation and the most urgent and widely supported area for cooperation.

Specifically, companies are calling for:

- Common definitions, timelines and thresholds;
- Support for national and international cyber regulators' forums to harmonise reporting requirements;
- Greater interoperability in timelines, thresholds, formats and portals for incident reporting;
- Initial notifications limited to essential information;
- A consistent approach by authorities to protecting information submitted in good faith, for example statutory confidentiality safeguards, proportionate liability protections and controlled onward sharing.

2. Align on risk-based outcomes

Companies look to regulators to adopt risk-based and outcome-based approaches, giving organisations flexibility to achieve objectives efficiently. Companies emphasise:

- Requirements should be targeted and proportionate to risk, technically feasible, and focused on measurable security outcomes;
- To avoid uncertainty undermining investment in cyber defence and security, supply chain measures should be based on proportionate, evidence-based risk assessments rather than automatic technology restrictions;
- Policymakers should consider operational impacts, replacement feasibility, investment cycles and service continuity, while respecting national security responsibilities.

3. Reduce duplication through mutual recognition

Aligning cybersecurity policy with international standards, where possible, would reduce the need for firms to repeat substantially similar assessments in every jurisdiction. Specifically, companies are calling for:

- Mutual recognition of cybersecurity labels to reduce duplicative compliance requirements, promote interoperability, and serve as a model for international regulatory cooperation;
- Mutual recognition of certifications, allowing one certification, audit or assessment to count across jurisdictions;
- Cybersecurity certification remaining voluntary unless a clearly demonstrated sector-specific risk justifies otherwise.

4. Improve capacity building

Structural gaps in the cybersecurity workforce increase the effects of fragmentation, and companies need policy responses to treat the underlying skills shortage as part of the solution. Companies recommend that policymakers:

- Take action to address the need for cybersecurity skills and respond to the labour market demand for this rapidly growing sector in partnership with the private sector;
- Expand the analytical and empirical evidence on this subject to enable more efficient policy responses to address capacity shortages in this industry;
- Introduce targeted tax exemptions and financial incentives for cybersecurity investments, specifically designed to support SMEs in overcoming resource constraints, adopting secure technologies, and achieving regulatory compliance.

5. Ensure early and structured business engagement

Business experience is an important source of evidence in developing practical solutions for advancing regulatory coherence that can support effective cyber defence. Business calls for:

- The OECD to serve as a forum for a regular dialogue between business and regulators to advance evidence-based solutions for greater cybersecurity regulatory coherence.

Mobilising the OECD

Cybersecurity is a shared challenge that needs greater international coordination to complement the existing efforts at national and regional levels. Enabling greater coherence in cybersecurity regulation would improve security outcomes while reducing unnecessary economic costs and frictions.

As a trusted multilateral forum, the OECD is well placed to convene regulators, help build the multidisciplinary evidence base, and support the development of practical guidance toward greater interoperability for cybersecurity rules.

In this spirit, Business would welcome OECD engagement across three areas: helping to build the evidence base, convening regulators in structured dialogue, and supporting the development of practical guidance. Specifically, Business recommends that the OECD:

Build the evidence base

- **Map the cybersecurity regulatory landscape** to identify overlapping and conflicting requirements;
- **Measure the economic impact** and cost of cybersecurity regulatory fragmentation;
- **Take stock of how incidents are being handled** and develop a common form for incident reporting, covering taxonomies, thresholds, definitions and interoperable timelines;
- **Identify best practices** for mutual recognition approaches to enhance coherence of cybersecurity regulatory frameworks.

Convene stakeholders

- **Leverage its convening power to facilitate a regular structured dialogue** among cybersecurity regulators and policymakers with the private sector at CISO level and relevant stakeholders across jurisdictions to exchange experience, identify challenges and advance best practice;
- **Engage with relevant global fora** such as the G7/G20 and regional models such as the EU, APEC, and ASEAN and reach out to OECD non-members through regional networks.

Develop practical guidance

- **Consider dedicated guidance to advance cybersecurity regulatory coherence** and interoperability in the development and implementation of laws, building upon the OECD Digital Security Recommendations, particularly as related to supply-chain requirements for SMEs and critical sectors;
- **Identify and respond to capacity shortages** through cross-cutting OECD work including related to skills and labour market issues;
- **Promote adequately resourced and technically independent cybersecurity institutions** that complement national authorities and support international coordination, interoperability and trust.

Sustained OECD engagement on cybersecurity regulatory fragmentation can help shift the focus and resources of the businesses at the front lines of cyber defence from compliance and towards effective, risk-based cyber resilience.

Engaging sectoral bodies would further ensure that industries facing extensive cybersecurity obligations without a dedicated sectoral cyber regulator are represented in this dialogue. Business looks to governments to resource and empower the OECD to advance an ambitious agenda on cybersecurity regulatory coherence that delivers practical solutions for reducing complexity, boosting confidence and capacity for effective and efficient cyber defence.

Conclusion

Cybersecurity is, above all, a global challenge. Attackers operate across borders, and an incident that starts in one jurisdiction can spread through supply chains, networks and services in many others. In response, cyber-defence works best when organisations and authorities can share information and coordinate on the same scale.

Growing fragmentation and complexity across cybersecurity regulatory frameworks are creating significant compliance burdens, diverting resources from managing cyber risks and rapidly evolving cyber threats. Fragmentation and complexity across cybersecurity regulatory frameworks are creating significant compliance burdens and diverting resources from managing cyber risk at a time of rapidly evolving threats. Regulatory coherence and interoperability serve a double purpose: they reduce unnecessary costs for business but they also strengthen collective cybersecurity resilience, critical infrastructure protection, economic growth and national security.

Addressing these challenges requires sustained and meaningful multistakeholder dialogue including business and the relevant policymakers. The OECD should play a critical role as a trusted forum for this dialogue, bringing governments, regulators and business together to enhance regulatory coordination, identify and exchange good practices, and develop more consistent and interoperable approaches, to focus resources on effectively managing cyber risk and strengthening collective resilience.

References

1. DIGITALEUROPE, "The imperative of global harmonisation of cybersecurity rules for collective defence", 2025.
2. Chief Information Security Officers, "CISO Letter to G7 and OECD on Cybersecurity Regulatory Fragmentation", April 2025.
3. Alexander Evans and Pierre Noro (London School of Economics and Sciences Po), "Defragmenting International Cyber Security Regulations", April 2026.
4. Ibid.
5. IBM, "Cost of a Data Breach Report 2024", July 2024.
6. World Economic Forum, "The pace of innovation is speeding up. Digital fragmentation threatens that", January 2024.
7. CITP, "Interoperability of Data Governance Regimes: Challenges for Digital Trade Policy"
8. Ibid.
9. Cybersecurity Tech Accord, "Advancing International Alignment in Cybersecurity Regulation to Strengthen Collective Resilience", statement, 25 March 2026.
10. Josephine Wolff, "International Cybersecurity Regulatory Harmonization: Opportunities for Reciprocity and Mutual Recognition among G7 and Quad Countries", Working Paper, Fletcher School of Law and Diplomacy (Tufts University), Hitachi Center for Technology and International Affairs, March 2026.
11. *Business at OECD* (BIAC), "Survey Addressing: Regulatory Fragmentation as an Obstacle to Cyber Resilience", member survey, 2026.
12. Office of the National Cyber Director (ONCD), The White House, "Summary of the 2023 Cybersecurity Regulatory Harmonization Request for Information", June 2024.
13. Ibid.
14. GSMA, "Impact of Cybersecurity Regulation on Mobile Operators", November 2025.

Business at OECD (BIAC) National Members

Australia	**ACCI: Australian Chamber of Commerce and Industry**
Austria	**IV: Federation of Austrian Industries**
Belgium	**VBO FEB: Federation of Belgian Enterprises**
Canada	**Canadian Chamber of Commerce**
Chile	**CPC: Confederation of Production and Commerce of Chile**
Colombia	**ANDI: National Business Association of Colombia**
Costa Rica	**UCCAEP: Costa Rican Union of Chambers and Associations of the Private Business Sector**
Costa Rica	**CICR: Chamber of Industries of Costa Rica**
Czech Republic	**SP: Confederation of Industry of the Czech Republic**
Denmark	**DA: Danish Employers' Confederation**
Denmark	**DI: Confederation of Danish Industry**
Estonia	**Estonian Employers' Confederation**
Finland	**EK: Confederation of Finnish Industries**
France	**MEDEF: Movement of the Enterprises of France**
Germany	**BDA: Confederation of German Employers' Associations**
Germany	**BDI: Federation of German Industries**
Greece	**SEV: Hellenic Federation of Enterprises**
Hungary	**MGYOSZ: Confederation of Hungarian Employers and Industrialists**
Hungary	**VOSZ: Confederation of Hungarian Business**
Iceland	**SA: Confederation of Icelandic Enterprise**
Ireland	**Ibec: Irish Business and Employers Confederation**
Israel	**MAI: Manufacturers' Association of Israel**
Italy	**assonime: The Association of Italian Joint Stock Companies**
Italy	**CONFINDUSTRIA: General Confederation of Italian Industry**
Italy	**FeBAF: Italian Banking Insurance and Finance Federation**
Japan	**Keidanren: Japan Business Federation**
Korea	**FKI: Federation of Korean Industries**
Latvia	**LDDK: Employers' Confederation of Latvia**
Lithuania	**LPK: Lithuanian Confederation of Industrialists**
Luxembourg	**FEDIL: The Voice of Luxembourg's Industry**
Mexico	**COPARMEX: Employers Confederation of the Mexican Republic**
Netherlands	**VNO-NCW: Confederation of Netherlands Industry and Employers**
New Zealand	**BusinessNZ**
Norway	**NHO: Confederation of Norwegian Enterprise**
Portugal	**CIP: Confederation of Portuguese Business**
Poland	**Polish Confederation Lewiatan**
Slovakia	**RÚZ: Slovak Employers' Federation**
Slovenia	**ZDS: Association of Employers of Slovenia**
Spain	**CEOE: Confederation of Employers and Industries of Spain**
Sweden	**Svenskt Näringsliv: Confederation of Swedish Enterprise**
Switzerland	**economiesuisse: Swiss Business Federation**
Switzerland	**Swiss Employers Confederation**
Türkiye	**TİSK: Turkish Confederation of Employer Associations**
Türkiye	**TOBB: Union of Chambers and Commodity Exchanges of Türkiye**
Türkiye	**TÜSIAD: Turkish Industry and Business Association**
United Kingdom	**CBI: Confederation of British Industry**
United States	**USCIB: United States Council for International Business**

(This page has been intentionally left blank)

BUSINESS at OECD | Business and Industry Advisory Committee to the OECD

Established in 1962, *Business at OECD* (BIAC) is the officially recognised institutional business voice at the OECD. We stand for policies that enable businesses of all sizes to contribute to economic growth, sustainable development, and societal prosperity. Through *Business at OECD*, national business and employers' federations representing over 10 million companies provide perspectives to cutting-edge OECD policy debates that shape market-based economies and impact global governance. Our expertise is enriched by the contributions of a wide range of international sector organisations.

Business at OECD (BIAC)
13/15 Chaussée de la Muette
75016 Paris, France

www.businessatoecd.org
@BusinessatOECD
Business at OECD

Tel: +33 (0)1 42 30 09 60
communications@biac.org

Restricted Use - À usage restreint