

January  
2024

# GUARDING GLOBAL COMMERCE

How Cybersecurity is  
Addressed in International  
Trade Agreements



# Introduction

Our global economy is underpinned by digital systems needed to deliver products and services and conduct business with customers around the world, thus, cybersecurity has become foundational to international trade. Trust in digital systems fortifies the ability of every country to promote consumer confidence and participation in the digital economy.

Cybersecurity itself is a fundamentally global issue with cyber-attacks being launched across borders, often leveraging infrastructure in multiple jurisdictions to conduct a single attack. To respond to these threats effectively, organizations must be able to move certain data across borders and implement risk management best practices consistently in each jurisdiction in which they operate.

The increasingly fragmented state of global cyber regulation undermines cybersecurity and the growth potential of digital trade. Trade agreements represent one key forum for addressing this fragmentation by enabling governments to align themselves with best practices, enhancing cybersecurity and avoiding the establishment of non-tariff barriers to trade.

The Coalition to Reduce Cyber Risk (CR2) is committed to promoting best-in-class approaches to cybersecurity risk management. As part of this commitment, this paper outlines the benefits of incorporating cybersecurity provisions into free trade agreements (FTAs) through an overview of the 11 FTAs that have incorporated cybersecurity provisions to-date. It categorizes these provisions into 8 distinct areas and analyzes the commonalities and differences in how they are addressed. Finally, it provides recommendations as to how future trade agreements can build upon the foundations that have been laid since the first mention of cybersecurity in trade agreements in 2018.

It is our hope that this paper can serve as a resource to policymakers and trade negotiators, enabling them to understand why cybersecurity should be addressed in trade agreements and how other countries have done so.



# The benefits of **ADDRESSING CYBERSECURITY IN TRADE AGREEMENTS**



In an increasingly digitized world, international trade agreements have evolved to address the critical issue of cybersecurity. The integration of cybersecurity principles into these agreements offers a multitude of benefits, not only for industry but also for governments and consumers. This section explores the advantages of incorporating cybersecurity considerations into international trade agreements and emphasizes the importance of aligning policies with best practices and consensus standards.

## **Cybersecurity enhances consumers' trust in digital systems and increases digital trade.**

Cybersecurity plays a pivotal role in enhancing trust within digital systems, a trust that serves as the cornerstone for leveraging digital ecosystems in the realm of commerce. The failure to adequately protect consumers and maintain the availability of networks can significantly erode confidence in digital trade and e-commerce.<sup>1</sup> Policies that hinder companies from adopting a risk management-based approach not only undermine the resilience and availability of digital systems, but also risk limiting the effectiveness of companies in safeguarding these systems. In particular, prescriptive policies that deviate from established cybersecurity best practices further exacerbate these limitations, potentially leaving digital systems vulnerable to threats.



1. Atlantic Council, Report of the Commission on the Geopolitical Impacts of New Technologies, and Data: Chapter 3. Enhanced trust and confidence in the digital economy, <https://www.atlanticcouncil.org/content-series/geotech-commission/chapter-3/> (Last accessed Oct. 16, 2023.)

## Unnecessary divergence in policymaking inhibits market access and competition.

Unnecessary policy divergence in the regulatory landscape poses a significant threat, diminishing both market access and competition. Governments have the opportunity to address common regulatory objectives in a manner that does not restrict trade by adopting a risk-based approach and implementing consensus standards. However, when governments mandate policies that deviate from this approach, they run the risk of creating a web of inconsistent, redundant, or conflicting legal requirements which can have profound implications and costs for companies. These conflicting legal requirements act as a non-tariff barrier, forcing companies into the burdensome position of assessing whether these requirements are redundant or substantively different.<sup>2</sup>

The fear of legal risk may even drive companies to exit a market altogether. The cumulative effect of these policies is the stifling of competition and trade, which not only diminishes the value proposition for consumers but also threatens the integrity of security operations.

Critical infrastructure operators are burdened with managing the cost and complexity of complying with redundant, inconsistent, and/or conflicting security measures composed by local cybersecurity laws that share the overall same objective.



2. The Organization for Economic Cooperation and Development (OECD), *Fostering Economic Resilience in a World of Open and Integrated Markets*, <https://www.oecd.org/newsroom/OECD-G7-Report-Fostering-Economic-Resilience-in-a-World-of-Open-and-Integrated-Markets.pdf> (Last accessed Oct. 16, 2023).


## The use of consensus standards reduces regulatory complexity and facilitates multi-country supply chains.



The adoption of consensus standards serves as a powerful tool in mitigating regulatory complexity while concurrently streamlining the operation of multi-country supply chains. By consistently implementing these consensus-based standards on an international scale, a level playing field is established, ensuring equal access for companies irrespective of their country of origin. The alignment of national policies with these globally recognized standards substantially reduces complexity for small and medium-sized enterprises (SMEs), enabling them to seamlessly integrate into global supply chains.<sup>3</sup> Furthermore, when countries adhere to the same set of standards, vendors are able to sell their products and services to customers with heightened efficiency, resulting in more streamlined and effective trade practices.



<sup>3</sup>. International Telecommunication Union (ITU), Brokering standards by consensus, <https://www.itu.int/en/mediacentre/backgrounders/Pages/standardization.aspx> (Last accessed Oct. 16, 2023).



## Trade commitments on cybersecurity support small and medium-sized entities (SMEs).

Trade commitments on cybersecurity offer substantial support to small and medium-sized entities (SMEs) by streamlining supply chain integration, promoting information sharing, and yielding enhanced security outcomes. An aligned approach in trade agreements elevates SMEs participating in the market, in turn both fostering healthy competition and welcoming new market entrants. Conversely, regulatory divergence forces suppliers into an intricate decision making process - complying domestically, aligning with international best practices, or incurring duplicative compliance costs.<sup>4</sup> This divergence also compels purchasers to make challenging choices, either excluding capable vendors from their supply chain or straying from their established security standards.

The consistent adoption of standards not only reduces complexity but also reduces compliance costs for SMEs. Moreover, the incorporation of cybersecurity principles into trade agreements serves to clearly demonstrate best practices for

non-governmental stakeholders. By avoiding the need to adhere to divergent regulatory regimes, smaller companies experience reduced operational complexity, a critical factor when confronting cyber threats. The “conform once, comply many” approach significantly alleviates compliance costs for businesses, an especially pertinent issue for SMEs struggling to bear the expenses associated with complying with multiple regulatory regimes. Furthermore, alignment with international best practices leads to improved security outcomes, with vendors and operators setting expectations among their suppliers regarding the most effective international standards and best practices. This requirement for alignment incentivizes investment in crucial areas such as workforce development, education and training, penetration testing. Once integrated into the supply chain, vendors are more likely to access valuable threat intelligence and receive ongoing support from more sophisticated vendors, further enhancing cybersecurity measures and bolstering overall resilience.



4. The European Union Agency for Cybersecurity (ENISA), Cybersecurity for SMEs: Challenges and Recommendations, June 28, 2021, <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>.

# Overview of TRADE AGREEMENTS

For our analysis, we identified every existing trade agreement that incorporated provisions pertaining to cybersecurity. In total 11 free trade agreements, digital economy agreements, or economic partnership agreements qualified. These incorporated 22 countries from five regions: Asia, Europe, North America, Oceania, and South America.

Year	Agreement	Participants
2018	Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)	<ul style="list-style-type: none"> <li>• Australia</li> <li>• Brunei</li> <li>• Canada</li> <li>• Chile</li> <li>• Chile</li> <li>• Japan</li> <li>• Malaysia</li> <li>• Mexico</li> <li>• New Zealand</li> <li>• Peru</li> <li>• Singapore</li> <li>• Vietnam</li> </ul>
2018	US-Mexico-Canada Agreement (USMCA)	<ul style="list-style-type: none"> <li>• Canada</li> <li>• Mexico</li> <li>• USA</li> </ul>
2019	US-Japan Digital Trade Agreement (USJDTA)	<ul style="list-style-type: none"> <li>• Japan</li> <li>• USA</li> </ul>
2020	Regional Comprehensive Economic Partnership (RCEP)	<ul style="list-style-type: none"> <li>• Australia</li> <li>• Brunei</li> <li>• Cambodia</li> <li>• China</li> <li>• Indonesia</li> <li>• Japan</li> <li>• Korea</li> <li>• Laos</li> <li>• Malaysia</li> <li>• Myanmar</li> <li>• New Zealand</li> <li>• Philippines</li> <li>• Singapore</li> <li>• Thailand</li> <li>• Vietnam</li> </ul>
2020	Digital Economy Partnership Agreement (DEPA)	<ul style="list-style-type: none"> <li>• Chile</li> <li>• New Zealand</li> <li>• Singapore</li> </ul>
2020	Singapore-Australia Digital Economy Agreement (SADEA)	<ul style="list-style-type: none"> <li>• Australia</li> <li>• Singapore</li> </ul>
2021	Australia-UK Free Trade Agreement (A-UKFTA)	<ul style="list-style-type: none"> <li>• Australia</li> <li>• UK</li> </ul>
2022	Korea-Singapore Digital Partnership Agreement (KSDPA)	<ul style="list-style-type: none"> <li>• Korea</li> <li>• Singapore</li> </ul>
2022	UK-Singapore Digital Economy Agreement (UKSDEA)	<ul style="list-style-type: none"> <li>• Singapore</li> <li>• UK</li> </ul>
2022	New Zealand-UK Free Trade Agreement (NZ-UK FTA)	<ul style="list-style-type: none"> <li>• New Zealand</li> <li>• UK</li> </ul>
2023	EU-New Zealand Free Trade Agreement (EU-NZ FTA)	<ul style="list-style-type: none"> <li>• New Zealand</li> <li>• EU</li> </ul>

# DETAILED ASSESSMENT OF CYBER COMPONENTS

For each of the 11 trade agreements, we categorized and assessed the various cybersecurity components that have appeared or been proposed in negotiations, whether each agreement incorporates each component, and what language it uses to do so. The identified cyber components range from establishing a basic connection between cybersecurity and trade all the way to agreeing to accept mutual recognition of cybersecurity baselines.

While there is some variation in how cybersecurity is addressed in the trade agreements, many components are consistent across agreements involving countries from different regions and different stages of development. The general trend over time has been towards incorporating more components into each trade agreement.

	2018	2019	2020	2021	2022	2023					
	CPTPP	USMCA	USJDTA	RCEP	DEPA	SADEA	A-UKFTA	KDSPA	UKSDEA	NZ-UK FTA	EU-NZ FTA
Establish Cyber-Trade Link	✗	✓	✓	✗	✓	✓	✓	✓	✓	✓	✓
Government Capacity Building	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
International Operational Collaboration	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗
Workforce Development Collaboration	✗	✗	✗	✗	✓	✓	✓	✓	✓	✓	✗
Risk-based Approaches to Cybersecurity	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗
Use of Industry Standards	✗	✓	✓	✗	✗	✗	✓	✗	✓	✓	✗
Common Regulatory Baselines for IoT	✗	✗	✗	✗	✗	✗	✗	✗	✓	✗	✗
Coordinated Vulnerability Disclosure	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗

This illustration captures the different components that have been included in prominent trade agreements to-date





# 1. ESTABLISH CYBER-TREADE LINK

**Definition:** The trade agreement acknowledges a connection between cybersecurity and digital trade or the digital economy.

## MODEL A

“The parties recognize that threats to cybersecurity undermine confidence in digital trade.”

## MODEL B

“The parties [have a shared vision to promote/recognize the importance of promoting] secure digital trade to achieve global prosperity and recognize that cybersecurity underpins the digital economy.”

## MODEL C


“The parties recognize the importance of cooperating on cybersecurity matters relevant to digital trade.”

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		None
2018	USMCA		Model A <sup>5</sup>
2019	USJDTA		Model A <sup>6</sup>
2020	RCEP		None
2020	DEPA		Model B <sup>7</sup>

5. Office of the United States Trade Representative (USTR), US-Japan Trade Agreement Text, Oct. 7, 2019, <https://ustr.gov/countries-regions/japan-korea-apec/japan/us-japan-trade-agreement-negotiations/us-japan-trade-agreement-text>.

6. USTR, Agreement Between the United States of America, the United Mexican States, and Canada, July 1, 2023, <https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between>

7. New Zealand Foreign Affairs and Trade, DEPA text and resources, <https://www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/digital-economy-partnership-agreement-depa/depa-text-and-resources/> (Last accessed Oct. 16, 2023).

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2020	SADEA		<b>Model B<sup>8</sup></b>
2021	A-UKFTA		<b>Model A<sup>9</sup></b>
2022	KSDPA		<b>Model B<sup>10</sup></b>
2022	UKSDEA		<b>Model B<sup>11</sup></b>
2022	NZ-UK FTA		<b>Model B<sup>12</sup></b>
2023	EU-NZ-FTA		<b>Model C<sup>13</sup></b>



9 of the 11 trade agreements establish a link between cybersecurity and digital trade or the digital economy, including the last 7 to be signed.

Model A, favored by the US, has not appeared in a trade agreement since 2019, though this is most likely due to the fact that the US has not signed a trade agreement since then. Model B, favored by Singapore, has become increasingly common, featuring in 5 of the last 7 trade agreements to be signed. Model C, preferred by the EU, has only appeared in one trade agreement.

While Model B is slightly more comprehensive in highlighting both the cyber-trade link and the importance of securing digital trade, the differences in the 3 models do not substantively alter the impact of the agreement.

8. Australian Government Department of Foreign Affairs and Trade, Australia-Singapore Digital Economy Agreement, Dec. 8, 2020, <https://www.dfat.gov.au/trade/services-and-digital-trade/australia-and-singapore-digital-economy-agreement>.
9. Australian Government Department of Foreign Affairs and Trade, Australia-UK FTA Official Text, <https://www.dfat.gov.au/trade/agreements/in-force/aukfta/official-text> (Last accessed Oct. 16, 2023).
10. Ministry of Trade and Industry Singapore, Korea-Singapore Digital Partnership Agreement (KSDPA), Nov. 21, 2022, <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/KSDPA>.
11. Ministry of Trade and Industry Singapore, UK-Singapore Digital Economy Agreement (UKSDEA), Feb. 25, 2022, <https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/UKSDEA>.
12. Gov.uk, UK/New Zealand: Free Trade Agreement, Oct. 27, 2022, <https://www.gov.uk/government/publications/uknew-zealand-free-trade-agreement-cs-new-zealand-no12022>.
13. European Commission, EU-New Zealand: Text of the Agreement, July 9, 2023, [https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement\\_en](https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/new-zealand/eu-new-zealand-agreement/text-agreement_en).

## 2. GOVERNMENT CAPACITY BUILDING

**Definition:** The trade agreement promotes government capacity for the purposes of cyber incident response.

### MODEL A




“The parties recognize the importance of building the capabilities of their government agencies responsible for computer security incident response.”

### MODEL B

“Accordingly the parties shall endeavor to build the capabilities of their respective national entities responsible for cybersecurity incident response.”



	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		Model A
2018	USMCA		Model B
2019	USJDTA		Model B
2020	RCEP		Model A
2020	DEPA		Model A
2020	SADEA		Model A
2021	A-UKFTA		Model B
2022	KSDPA		Model A

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2022	UKSDEA		<b>Model A</b>
2022	NZ-UK FTA		<b>Model A</b>
2023	EU-NZ-FTA		<b>None</b>

## Analysis

Including language on government capacity building in the context of cybersecurity services is one of the only identified components that is present in almost all selected trade agreements. In total, 10 of the 11 trade agreements incorporate either the Model A or Model B approach.

While the language in Model B is relatively weak within trade parlance, it is stronger than Model A, in that it places on signatories an obligation to “endeavor to” build the capabilities of their national entities. Model A, conversely, merely notes that the importance of doing so.

Interestingly, we see here that CPTPP, which did not establish a clear link between cyber and trade, actually has one of the strongest provisions for cybersecurity capacity building. Additionally, it is evident again that the trade agreements do not necessarily include stronger cybersecurity provisions as time progresses, as Model A has become more prevalent in recent years. The most recent agreement, EU-NZ NFTA, does not include any language on capacity building.





### 3. INTERNATIONAL OPERATIONAL COLLABORATION

**Definition:** The trade agreement calls for the use of (new, strengthened, or existing) government-to-government cooperation mechanisms for the identification and mitigation of malicious cyber activity.

**MODEL A**

“The parties recognize the importance of using existing collaboration mechanisms to cooperate to identify and mitigate malicious intrusions or disseminations of malicious code that affect the electronic networks of the parties.”

**MODEL B**

“The parties shall endeavor to strengthen existing collaboration mechanisms for cooperating to identify and mitigate malicious intrusions or dissemination of malicious code that affect electronic networks, and use those mechanisms to swiftly address cybersecurity incidents, as well as for the sharing of information for awareness and best practices.”









**MODEL C**

“The parties recognize the importance of using existing collaboration mechanisms to cooperate on matters related to cybersecurity.”

**MODEL D**

“The parties further recognize the importance of using and strengthening existing collaboration mechanisms for cooperating to anticipate, identify, and mitigate malicious intrusions or dissemination of malicious code that affect the electronic networks of the Parties, and using those mechanisms to swiftly address cyber security incidents; and maintaining a dialogue on matters related to cyber security, including for the sharing of information and experiences for awareness and best practices.”

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		<b>Model A</b>
2018	USMCA		<b>Model B</b>
2019	USJDTA		<b>Model B</b>

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2020	RCEP		<b>Model C</b>
2020	DEPA		<b>Model A</b>
2020	SADEA		<b>Model A</b>
2021	A-UKFTA		<b>Model D</b>
2022	KSDPA		<b>Model A</b>
2022	UKSDEA		<b>Model D</b>
2022	NZ-UK FTA		<b>Model D</b>
2023	EU-NZ-FTA		<b>None</b>

## Analysis

Including a provision on international operational collaboration for the purposes of cybersecurity is the only other widely adopted cybersecurity provision among international trade agreements, with 10 out of the 11 agreements including some kind of commitment to international collaboration.

While Model A, favored by Singapore, sets reasonable parameters for international collaboration on identifying and mitigating malicious intrusions, Model B and Model D, favored by U.S. and U.K. respectively, take

things a step further and includes language on the sharing of information and best practices among international partners.

The varying degrees to which states include provisions on international collaboration is demonstrative of the difficulty trade agreements have in finding consensus among states on cybersecurity issues. The core language on international collaboration is shared across the agreements but diverges at the level of specificity and commitment to these principles and how the agreement will carry them out.



## 4. WORKFORCE DEVELOPMENT COLLABORATION

**Definition:** The trade agreement acknowledges the importance of workforce development and highlights opportunities for collaboration.

### MODEL A

“The parties recognize the importance of workforce development in the area of cybersecurity, including possible initiatives relating to mutual recognition of qualifications, diversity and equality.”






### MODEL B

“The Parties further recognize the importance of workforce development in the area of cybersecurity, including through possible initiatives relating to the training and development of youths, improving diversity and mutual recognition of qualifications.”

### MODEL C

“Accordingly, the Parties recognize the importance of workforce development in the area of cyber security, including through possible initiatives relating to training and development.”

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		None
2018	USMCA		None
2019	USJDTA		None
2020	RCEP		None
2020	DEPA		Model A
2020	SADEA		Model A

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2021	A-UKFTA		<b>Model A</b>
2022	KSDPA		<b>Model B</b>
2022	UKSDEA		<b>Model C</b>
2022	NZ-UK FTA		<b>Model A</b>
2023	EU-NZ-FTA		<b>None</b>

## Analysis

6 out of 11 trade agreements include a provision acknowledging the importance of cybersecurity workforce development.

Model A and Model B are similar in that they both recognize the importance of developing the cybersecurity workforce and include possible initiatives for the mutual recognition of qualifications, and diversity. Model B, however, specifically mentions the training and development of youths in relation to the cybersecurity workforce. While Model C makes no specific mention of diversity, but instead takes a high level approach

by citing initiatives related to general training and development.

The variations of a workforce provision in trade agreements demonstrates the difficulty in adopting identical language across agreements. When trade agreements adopt the same language on cybersecurity it enhances the international community's ability to interact seamlessly with other partners that are beholden to the same principles. Even slight changes in wording can affect the interoperability between nation states' cybersecurity operations and initiatives.





# 5. USE OF RISK-BASED APPROACHES TO CYBERSECURITY

**Definition:** The agreement recognizes the greater effectiveness of risk-based approaches and encourages parties to use them within their public and private sectors.



### MODEL A

“Given the evolving nature of cybersecurity threats, the Parties recognize that risk-based approaches may be more effective than prescriptive regulation in addressing those threats. Accordingly, each Party shall endeavor to employ, and encourage enterprises within its territory to use, risk-based approaches that rely on consensus-based standards and risk management best practices to identify and protect against cybersecurity risks and to detect, respond to, and recover from cybersecurity events.”









### MODEL B

“Given the evolving nature of cyber security threats, the Parties recognize that risk-based approaches may be more effective than prescriptive approaches in addressing those threats including in the context of digital trade. Accordingly, each Party shall encourage enterprises within its jurisdiction to use risk-based approaches that rely on open and transparent industry standards to:

- A** Manage cyber security risks and to detect, respond to, and recover from cybersecurity events; and
- B** Otherwise improve the cyber security resilience of these enterprises and their customers.”



	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		None
2018	USMCA		Model A
2019	USJDTA		Model A

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2020	RCEP		None
2020	DEPA		None
2020	SADEA		None
2021	A-UKFTA		Model A
2022	KSDPA		None
2022	UKSDEA		Model B
2022	NZ-UK FTA		Model B
2023	EU-NZ-FTA		None

## Analysis

5 out of 11 trade agreements recognize the greater effectiveness of risk-based approaches and encourage parties to use them within their public and private sectors.

While Model A and Model B each recognize that risk-based approaches are more effective than prescriptive regulation, they diverge at whether they encourage enterprises to use “consensus-based standards” or “open and transparent industry standards.” These two terms are often used interchangeably in colloquial language but refers to voluntary cybersecurity standards developed by international experts that designate risk reduction as the primary goal. A risk based approach builds the appropriate controls for the most severe vulnerabilities – prioritizing resources based on the level of concern. As opposed to a prescriptive, maturity-based approach that build capabilities to achieve a desired level of security.

The adoption of risk-based cybersecurity provisions in trade agreements has not seen linear success, but instead has been sporadically adopted throughout the agreements analyzed.

## 6. USE OF INDUSTRY STANDARDS



**Definition:** The trade agreement encourages parties to use of industry standards within their public and private sectors.

### MODEL A

“...each Party shall endeavor to employ, and shall encourage enterprises within its jurisdiction to use, risk-based approaches that rely on consensus-based standards...”

### MODEL B

“...each Party shall encourage enterprises within its jurisdiction to use risk-based approaches that rely on open and transparent industry standards...”

	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		None
2018	USMCA		Model A
2019	USJDTA		Model A
2020	RCEP		None
2020	DEPA		None
2020	SADEA		None
2021	A-UKFTA		Model A
2022	KSDPA		None
2022	UKSDEA		Model B
2022	NZ-UK FTA		Model B
2023	EU-NZ-FTA		None

## Analysis

6 of the 11 trade agreements encourage the use of industry standards within their public and private sectors.

The main differentiation in the language centers around whether to adopt “consensus-based standards” or “open and transparent industry standards”.

Despite being similar, “consensus-based standards” is more abstract while “open and transparent industry standards” affirms that the standards can be practically implemented by industry. It is important that cybersecurity standards have practical utility and are supported by the industry that will rely on them to guide cybersecurity risk management processes.












## 7. MUTUAL RECOGNITION OF BASELINE SECURITY STANDARDS FOR CONSUMER IOT

**Definition:** The trade agreement encourages the establishment of a mutual recognition agreement for baseline security standards in consumer IoT.

### MODEL A

“Accordingly, the Parties recognize the importance of establishing mutual recognition of a baseline security standard for consumer Internet of Things devices to raise overall cyber hygiene levels and better secure cyberspace domestically.”



	<i>Agreement</i>	<i>Countries</i>	<i>Approach</i>
2018	CPTPP		None
2018	USMCA		None
2019	USJDTA		None
2020	RCEP		None
2020	DEPA		None
2020	SADEA		None
2021	A-UKFTA		None
2022	KSDPA		None
2022	UKSDEA		Model A
2022	NZ-UK FTA		None
2023	EU-NZ-FTA		None

## Analysis

The Singapore-UK agreement is the only one of the identified trade agreements to include a cybersecurity provision relating to the use of common security baselines for regulatory approval. Setting common security baselines can help increase visibility into one's cybersecurity ecosystem and help ensure that all necessary data is protected. Sharing common cybersecurity baselines among the international community would strengthen the overall resiliency of the digital economy and increase interoperability between nation states. Trade agreements in the future should consider including common baselines for cybersecurity to bolster the economy's security posture and protect against malicious threat actors.

## 8. COORDINATED VULNERABILITY DISCLOSURE

**Definition:** The trade agreement encourages the adoption of coordinated vulnerability disclosure programs by the private sector.

### Analysis

The final identified cybersecurity component is the inclusion of a coordinated vulnerability disclosure component. These are voluntary processes that communicate the disclosure and receipt of a discovered cybersecurity vulnerability to those affected. While there have been no trade agreements to date that have included this component, we would encourage future agreements to adopt such provision. The U.S. government has taken significant steps to promote vulnerability disclosure by issuing draft regulations to require federal civilian agencies to adopt certain vulnerability disclosure processes<sup>14</sup> and by integrating these processes into the NIST Cybersecurity Framework.<sup>15</sup>

Cybersecurity vulnerabilities affect stakeholders across borders, but implementing vulnerability disclosure programs strengthens product resilience and trust, which in turn strengthens trust in the digital ecosystem.<sup>16</sup> Aligned vulnerability disclosure norms can also help address barriers to trade. Building the necessary governmental capacities to support a coordinated vulnerability disclosure program and encouraging the inclusion of such programs in international trade agreements is a good way to promote better cybersecurity management among the international community. Therefore, we would propose the following language be considered for future trade agreements:

#### **1. The Parties recognize that threats to cybersecurity undermine confidence in digital trade. Accordingly, the Parties shall endeavor to:**

- A.** Build the capabilities of national entities responsible for coordinated vulnerability disclosure; and
- B.** Establish processes for disclosure of “zero day” vulnerabilities from government to the private sector; and
- C.** Use and encourage industry to use voluntary processes for coordinated vulnerability disclosure aligned with international standards.

<sup>14</sup>. Cybersecurity & Infrastructure Security Agency (CISA), BOD 20-01: Develop and Publish a Vulnerability Disclosure Policy, Sep. 2, 2020, <https://www.cisa.gov/news-events/directives/bod-20-01-develop-and-publish-vulnerability-disclosure-policy>.

<sup>15</sup>. National Institute for Standards and Technology (NIST), Cybersecurity Framework, <https://www.nist.gov/cyberframework> (Last accessed Oct. 18, 2023).

<sup>16</sup>. Rapid7, Cybersecurity Vulnerability Disclosure in Trade Agreements, Mar. 24, 2020, <https://www.rapid7.com/blog/post/2020/03/24/cybersecurity-vulnerability-disclosure-in-trade-agreements/>.



# MOVING FORWARD

In the future, all forward-leaning trade agreements should look to incorporate these aforementioned cybersecurity principles. These principles represent a critical tool for driving adoption of consensus-based standards and risk management best practices that will enable a stronger global cybersecurity ecosystem overall. Strong cybersecurity enhances consumers' trust in digital systems and can increase digital trade, bolstering the international economy. Moving forward we recommend the following:

The international community should seek opportunities to increase collaboration mechanisms between the global cybersecurity community and various trade bodies. Increased collaboration could result in a unified approach to increasing cyber resiliency within trade negotiations.

Future trade agreements should promote, replicate, and expand impactful cybersecurity language included in previous agreements to date.

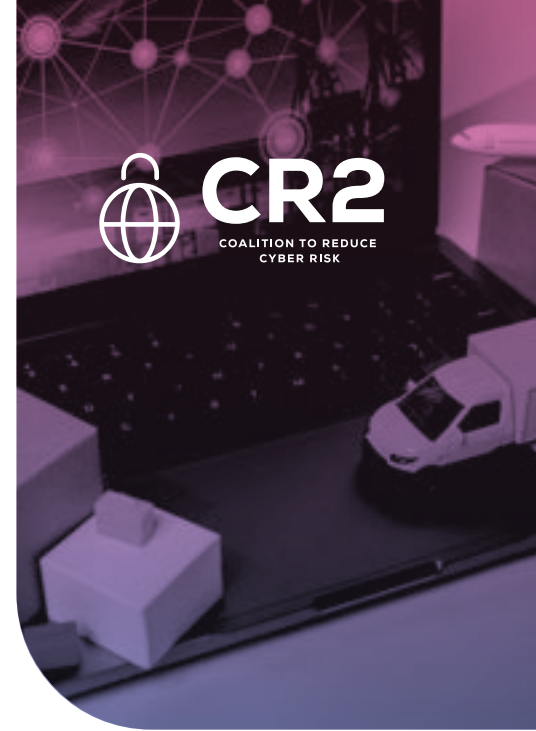
## CYBER IN SECURITY PARTNERSHIP

However, as demonstrated by our analysis, it is challenging to get repetitive adoption of strong cybersecurity provisions across multiple international trade agreements. The lack of ambition in trade agreements presents a stark distinction to the impressive progress made in security partnerships in the Indo-Pacific region. These include the Quadrilateral Security Dialogue, the trilateral summit among the US, Japan, and Republic of Korea, and the strengthening of a multitude of bilateral arrangements. The impressive progress and attention to cybersecurity within these multilateral diplomatic forums should be replicated and applied to trade. While USMCA might have set the standard for cybersecurity trade policy five years ago, it has since fallen behind. The Indo-Pacific region cannot rely solely on the burgeoning security umbrella as their economic dependence on China persists. Trade agreements are an important vehicle to promote stronger cybersecurity measures and can work in tandem with the increasing security partnerships to promote greater resilience in the region.

17. Wilson Center, The Indo-Pacific Region Needs a Comprehensive Digital Trade Agenda, Sep. 15, 2023, <https://www.wilsoncenter.org/article/indo-pacific-region-needs-comprehensive-digital-trade-agenda>.

Some of the hesitation in adopting stronger cybersecurity provisions in trade agreements center around the concern that it could lead to the outsourcing of domestic jobs. However, bolstering cybersecurity maturity can lead to having a comparative advantage in digital services (cloud, cybersecurity, etc.) which stimulates the economy and creates good paying jobs at home.

Moreover, digital trade agreements provide an opportunity for the collaborative championing of human rights and a model for digital governance grounded in the principles of a free, fair, and open internet. If democratic nations are not actively pursuing stronger cybersecurity measures in trade agreements, it will allow authoritarian regimes to strengthen and promote alternative models for digital governance. This is apparent with Russia's activities at the UN Cybercrime Convention negotiations<sup>18</sup> and the Chinese Data Security Law<sup>19</sup> that champions digital protectionism along with the rise of data localization measures.



## PROMOTE ROBUST CYBERSECURITY PRINCIPLES IN FUTURE TRADE AGREEMENTS

Moreover, a recent decision by the Office of the United States Trade Representative (USTR) to withdraw support for data free flows and data localization provisions at the World Trade Organization (WTO) e-commerce negotiations has sparked debates around promoting cross-border data flows. Increased data localization provisions reduce the holistic view that the security community has across its networks, infrastructure, endpoints, and partner ecosystems. A complete picture enables coordinated detection and response to threats across multiple regions, but as debates around on-premises solutions and data sovereignty persist, these cybersecurity capabilities to defend against malicious actors will be weakened.

These discussions will continue as the Indo-Pacific Economic Framework for Prosperity (IPEF) engages in its negotiations. IPEF was formed with 14 founding members of the Indo-Pacific region; Australia, Brunei Darussalam, Fiji India, Indonesia, Japan, the Republic of Korea, Malaysia, New Zealand, Philippines, Singapore, Thailand, and Vietnam.<sup>20</sup> These states have the ability to enhance and fortify the Indo-Pacific region's digital infrastructure by incorporating a strong, ambitious digital trade agenda that prioritizes cybersecurity into the framework. It would also reinforce the region's commitment to supporting an internet governance model based on freedom of speech, privacy, and security. Overall, the importance of cybersecurity in trade agreements cannot be understated. Future international trade agreements must prioritize robust cybersecurity provisions in order to secure the digital economy and to protect consumers.

18. Geneva Internet Platform, Key Takeaways from the Sixth UN Session on Cybercrime Treaty Negotiations, Sep. 13, 2023, <https://dig.watch/updates/key-takeaways-from-the-sixth-un-session-on-cybercrime-treaty-negotiations>.

19. Foreign Policy, Why China's New Data Security Law is a Warning for the Future of Data Governance, <https://foreignpolicy.com/2022/01/28/china-data-governance-security-law-privacy/> (Last accessed Oct. 18, 2023).

20. USTR, Indo-Pacific Economic Framework for Prosperity (IPEF), <https://ustr.gov/trade-agreements/agreements-under-negotiation/indo-pacific-economic-framework-prosperity-ipef> (Last accessed Oct. 18, 2023).





# CR2

COALITION TO REDUCE  
CYBER RISK

## **GUARDING GLOBAL COMMERCE**

**How Cybersecurity is  
Addressed in International  
Trade Agreements**