

April  
2023

**"BETTER  
CONNECTED: HOW  
CROSS-BORDER  
DATA FLOWS  
ENABLE STRONGER  
CYBERSECURITY"**



**CR2**  
COALITION TO REDUCE  
CYBER RISK



## About the coalition to reduce cyber risk (“CR2”)

CR2 members include global organizations that represent numerous sectors, including financial services, IT, and telecommunications, and that are committed to security, trust, and economic growth and opportunity. CR2 members have deep expertise in cybersecurity and enterprise risk management, as well as unique insights into cross-sector interdependences and global interconnectivity, which drive the need for consistent, foundational approaches to cybersecurity risk management across sectors and geographies. As such, CR2 has set out to work collaboratively with public and private sector entities in several dozen countries around the world to improve cybersecurity risk management practices that will both enhance cybersecurity and support economic growth.

### ABOUT THE CYBER RISK MANAGEMENT PLEDGE

In 2022, CR2 led the launch of the Cyber Risk Management Pledge, an initiative supported by more than 40 major companies and organizations from around the world. The Pledge highlighted the criticality of international standards and risk management -based approaches to ensuring seamless cyber resilience. For more information, please visit:

<https://www.crx2.org/pledge>

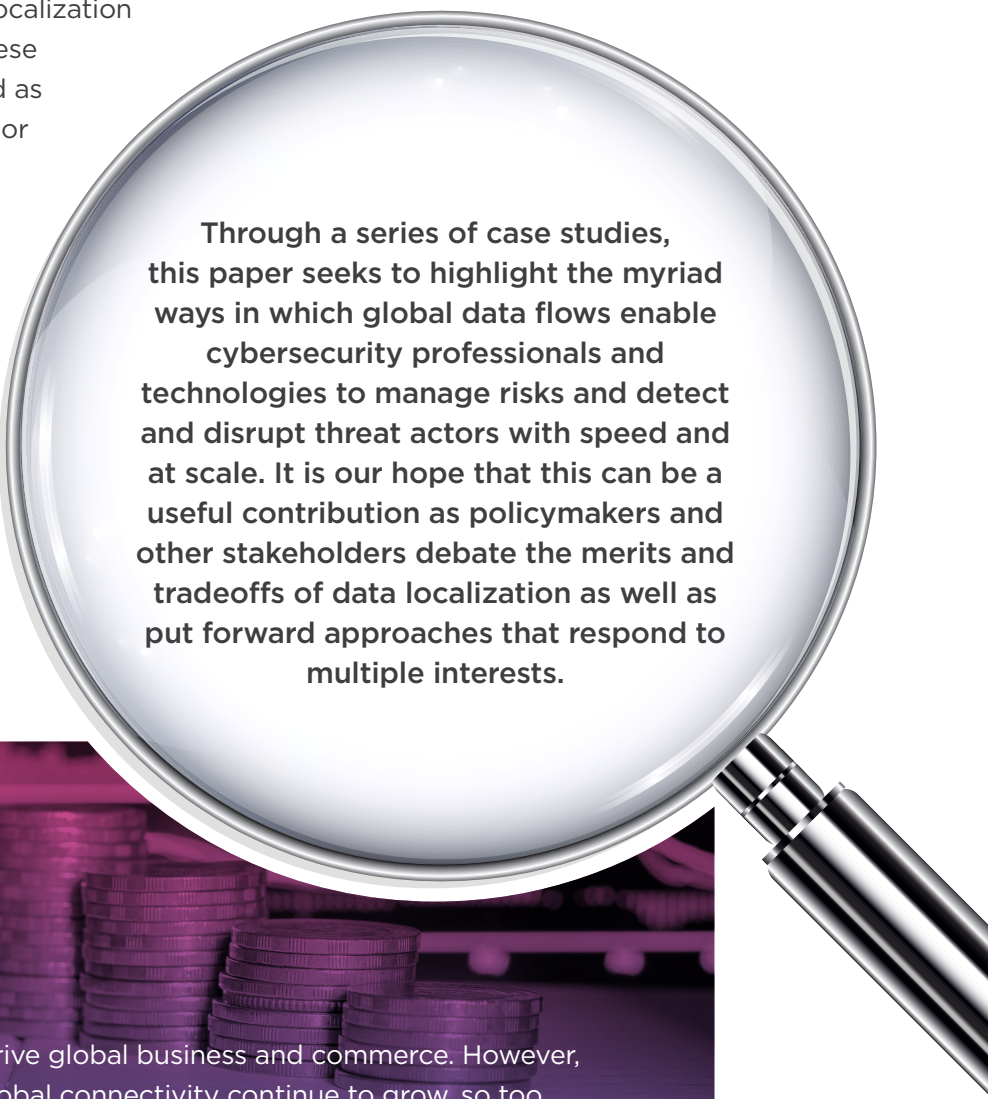


**CR2**  
COALITION TO REDUCE  
CYBER RISK

# How data flows support **CYBERSECURITY**



Data localization measures have been on the rise in recent years, with a majority of countries having implemented some form of localization requirements as of 2022.<sup>1</sup> These measures are often perceived as addressing privacy concerns or promoting local jobs. In the debates around these measures, however, the importance of global data flows to the international cybersecurity ecosystem has been largely under-discussed and underappreciated.



Through a series of case studies, this paper seeks to highlight the myriad ways in which global data flows enable cybersecurity professionals and technologies to manage risks and detect and disrupt threat actors with speed and at scale. It is our hope that this can be a useful contribution as policymakers and other stakeholders debate the merits and tradeoffs of data localization as well as put forward approaches that respond to multiple interests.



The internet and data flows drive global business and commerce. However, as the digital economy and global connectivity continue to grow, so too does the exposure to various cyber risks. Cybersecurity risk management is a critical way of reducing potential cybersecurity concerns and mitigating the negative impacts of digital insecurity on international trade.

**Ultimately, the promise of a safe and secure digital ecosystem is premised upon data flows that support cybersecurity activities.**

<sup>1</sup>. <https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/localization-of-data-privacy-regulations-creates-competitive-opportunities>

# INTRODUCTION

Cyber threats and defense are inherently global. Cyber threat actors are globally dispersed, and internationally coordinated. Their targets are often half a world away, and the infrastructure used to conduct malicious activities often weaves its way across dozens of international borders. Organizations managing cybersecurity risk also often have supply chains and operations that span across borders.

Key to combatting these cyber threats and managing cyber risks is the data – including security telemetry associated with the operation of technology products and systems – analyzed by defenders, including companies across all sectors. By leveraging cross-border data flows, security telemetry and broader threat intelligence and risk management data is allowed to be centralized, enabling providers to have a holistic view of threat activity and risk across their networks, infrastructure, endpoints, and partner ecosystem.

This holistic view enables coordinated detection and response across multiple regions, including the ability to discover, track, and mitigate global malicious activity. Increasingly, it also enables proactive blocking of attacks, as global data sets strengthen machine learning and AI-based cybersecurity capabilities. Additionally, it provides system optimization and overall efficiency by reducing the number of tools and systems needed to maintain and query complex data sets. The net result of these centralized capabilities is that global firms and providers are in a significantly stronger position to defend against and mitigate cyberthreats. In turn, those global firms can better protect themselves and their clients, enhance secure delivery of services, and improve their threat models and services going forward.







To illustrate how cybersecurity and resiliency benefits from open global data flows, we have compiled the following real-world case studies from our members. These examples form a non-exhaustive, but representative, sample of the types of activities powered by global flows of security telemetry and other cybersecurity risk management-enabling data. Each organization's varying networks, infrastructure, endpoints, partner ecosystems, and cybersecurity services mean that the types of data

on which it relies for cybersecurity protection and response – for its own ecosystem and that of its customers – may vary. However, data conveying typical behaviors of legitimate users, such as sign-in locations, often serves as context for anomalies. Such data might also be coupled with information about known threats and broader anomalies, such as direction to a new domain that's receiving very few other visitors – a strong indication of a malicious site.

## Preventing Credential Harvesting Attacks & Account Compromise



By volume, the largest security challenge facing companies – and the root cause behind almost all political campaign breaches over the last decade – is credential harvesting. These attacks make use of a variety of methods, such as phishing, to obtain valid credentials used to access a victims' networks and systems. To indicate the scale of the challenge, Microsoft's 2022 Digital Defense Report estimated that their systems block, on average, 710 million phishing emails per week.<sup>2</sup>



While victims of these attacks may reside within a given region, the attack and related malicious activity generally occurs globally and can only be seen globally. Combatting credential harvesting often requires the kinds of information only gleaned through permissive global data flows. For example, such information might lead to identifying someone connected from two locations at the same moment (e.g., simultaneously in the EU and Asia); identifying unusual patterns, such as checking email through an anonymized Brazilian VPN; and identifying anomalous patterns, such as navigating to a Canadian website nobody else visits. Some of the strongest security signals of credential harvesting activity comes from triangulating user activity around the world in a centralized fashion.

<sup>2</sup>. <https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report-2022>



## Financial Sector Fraud Prevention

Among the most significant threats to the financial sector is fraud. Reports suggest that it costs U.S. financial services and lending firms over \$4 for every \$1 of fraud loss, and that billions of dollars are lost each year globally.<sup>3,4</sup>

3, 4 Beyond the scale of the issue, fraudulent activities are increasingly becoming more sophisticated and complex with increased digitization and technology modernization.

Financial firms employ a multifaceted approach to counter fraud, and global data flows underpin the effectiveness of one of their most important tools: fraud detection models. The effectiveness of these models to accurately flag fraud is dependent on their ability to harness real-time data analysis of global data flows and be trained and fine-tuned on expansive global data sets. Limiting data sets and flows to particular regions or countries can blind these models to fraudulent patterns and strategies evolving in other parts of the world.

## Supply Chain Attack Recovery

Cyber supply chain attacks have gained notoriety in recent years with the widespread damage caused the SolarWinds and Kaseya VSA incidents. Unknown to many, global data flows played their part in limiting the harm caused. In the case of SolarWinds, one of the most sophisticated nation state attacks seen to date, a private company was able to identify a previously unknown variant of the malicious SolarWinds DLL. This information was used to inform response operations and mitigate damage. The key to this company's ability to identify this unknown variant is that many of their systems and tools, including AI/ML expert systems, file and content analysis, and executable behavioral analysis, operate and are trained over data from customers around the world. This company's security services process tens of trillions of signals every day, all of which helps to identify, investigate and automatically protect against malicious activity. Being able to process and learn from such signals in a centralized manner is a critical underpinning of this capability.

<sup>3</sup> <https://risk.lexisnexis.com/insights-resources/research/us-ca-true-cost-of-fraud-study#financialservices>

<sup>4</sup> <https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/financial-fraud-in-the-digital-space>



## Ransomware Attack Recovery

Ransomware continues to dominate global headlines as attacks by nation state and cybercriminal threat actors cripple governments and disrupt critical infrastructure.<sup>5,6</sup> Here too, global data flows help to enable more rapid and effective responses. A prominent example is the role of the private sector in mitigating the NotPetya ransomware worm. NotPetya, which emerged starting with a supply chain attack of the Ukrainian MeDoc software, leveraged previously unseen techniques and quickly spread to countless victims around the world. The incident spurred globally dispersed malware disassembly specialists into action, and they immediately began investigating this complex attack.

By leveraging data from impacted customers around the world, these specialists were able to understand the threat, and then contain it by immediately deploying new protections globally. Without the global security telemetry flows that allowed NotPetya's data to be aggregated, this work would have been slowed or made impossible. In short, global data flows may have significantly decreased total losses, which still accumulated to over one billion dollars.<sup>7</sup>

5. <https://www.wired.com/story/costa-rica-ransomware-conti/>
6. <https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf>
7. <https://www.cybereason.com/blog/notpetya-costs-companies-1.2-billion-in-revenue>
8. [https://blog.lumen.com/emotet-redux/?utm\\_source=referral&utm\\_medium=black+lotus+labs+page](https://blog.lumen.com/emotet-redux/?utm_source=referral&utm_medium=black+lotus+labs+page)
9. <https://www.netscout.com/blog/unrelenting-rise-botnets>
10. [https://blog.lumen.com/emotet-redux/?utm\\_source=referral&utm\\_medium=black+lotus+labs+page](https://blog.lumen.com/emotet-redux/?utm_source=referral&utm_medium=black+lotus+labs+page)
11. Ibid.
12. [https://blog.lumen.com/emotet-redux/?utm\\_source=referral&utm\\_medium=black+lotus+labs+page](https://blog.lumen.com/emotet-redux/?utm_source=referral&utm_medium=black+lotus+labs+page)

## Botnet Mitigation

Botnets remain an impactful if underappreciated cyber threat, with reports indicating that botnets continue to evolve and expand their capabilities.<sup>8,9</sup> Botnets with globally distributed nodes act as beachheads for later lateral movement within compromised device networks, and as a tool for spreading malware by “spamming targets through legitimate mail servers using stolen credentials.”<sup>10</sup> As above, global data flows contribute to mitigating this threat.

The private sector's effort against Emotet is a prime example. Emotet, one of the most notorious and prolific botnets, has “caused hundreds of millions of dollars in damage across critical infrastructure, healthcare, government organizations and enterprises around the world,” and as of early last year, was comprised of “approximately 130,000 unique bots spread across 179 countries.”<sup>11</sup> That information is known because security experts make use of global data flows to provide visibility into Emotet's infrastructure. This information is then leveraged to target and disrupt command and control devices “through take down notifications and null routing.”<sup>12</sup>

# Responding to War & Geopolitical Conflict

The unprovoked Russian invasion of Ukraine has illustrated how cross-border data flows strengthen cybersecurity and provide resilience from destructive attacks. Armed conflict that threatens critical services and infrastructure through either physical or cyber means is relatively common. Ukraine offers the best recent example of how modern conflicts increasingly require governments to be prepared to “disburse and distribute digital operations and data assets across borders and into other countries.”<sup>13</sup>

In the weeks leading up to the conflict, two U.S. companies contributed to safeguarding vital Ukrainian data by helping to transfer it to public cloud infrastructure located within Europe.<sup>14,15</sup> Once again, flows across all cloud-based infrastructure in the EU and of security telemetry globally played an essential role in allowing critical government services and functions to continue despite widespread cyber and physical attacks on the country’s “inhouse” infrastructure.



## Using AI to Block Wiper Attacks

In March 2022, a private company leveraged its AI capabilities to identify a wiper malware attack on a Ukrainian shipping company attributed to a Russian threat actor.<sup>16</sup> Wiper malware erases data and programs on the computer it infects, potentially disrupting both operations and continuity.

The first documented encounter of this malware was on a system running this company’s software with cloud protection enabled. Machine learning models, coupled with other client and cloud-based signals, enabled the company to block the wiper malware at first sight. Similarly, in 2021, this provider’s software, leveraging an AI pattern recognizer, blocked at first sight a file that was later confirmed as a variant of the GoldMax malware, which persists on networks by impersonating systems management software activities.<sup>17</sup>

<sup>13</sup>. <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-thecyber-war/>

<sup>14</sup>. <https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-its-present-andbuild-its-future>

<sup>15</sup>. <https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-thecyber-war/>

<sup>16</sup>. <https://www.armed-services.senate.gov/imo/media/doc/5.3.22%20Eric%20Horvitz%20Testimony.pdf>

<sup>17</sup>. <https://www.microsoft.com/security/blog/2021/07/27/combing-through-the-fuzz-using-fuzzy-hashingand-deep-learning-to-counter-malware-detection-evasion-techniques>



As cyber threat actors rapidly innovate, defenders must also invest in capabilities that allow them to act with greater scale and speed. For example, sophisticated threat actors can develop malware variants that allow them to circumvent cybersecurity technologies meant to block known malware, such as anti-virus protection products. However, leveraging AI technology dependent on being trained on and having continuous visibility into global data, defenders can block seeming malicious activity, such as malware variants, and update antivirus protections much more rapidly, reducing their impact.



For organizations to comprehensively manage risk, utilizing global data sets is essential for maintaining visibility and accurately understanding different risk scenarios. Limitations on cross-border data flows undermine integrated risk management practices by limiting capabilities to extract meaningful insights from local data. 7 Organizations have shifted to hosting complex data in repositories on the cloud and utilizing cloud providers' capabilities to provide faster and/or real-time analysis and reporting to address and inform business and

security considerations more dynamically. Restricting and localizing data sets and flows to particular regions leads to a fragmented view of risk considerations and thresholds, and ultimately limits an organization's ability to address firmwide enterprise risk.



# CONCLUSION

When discussing the role of global data flows, it can be easy, and even intuitive, to conclude that cybersecurity and resiliency are best served with walled gardens and strict data localization policies and laws. But this perception misses the critical role that global data flows play in bolstering cybersecurity and resiliency.

By providing examples of how global data flows contribute to countering account compromise, fraud, supply chain attacks, ransomware, botnets, and even the negative effects of war and geopolitical conflict – as well as how such flows enable the discovery and tracking of threat actors and the use of AI technologies that block threats at first sight – we hope to provide an important counterpoint to current data localization narratives.

We also hope to enliven the ongoing conversation initiated by the G7 on Data Free Flow with Trust, especially on how governments and private sector organizations can protect and even strengthen global flows of security telemetry and other cybersecurity-enabling data. We believe consistent approaches to cybersecurity risk management requirements, across both borders and sectors, are foundational to doing so. Where general data localization requirements are considered necessary, exemptions can be pursued to meet transparency and accountability as well as cybersecurity and resiliency imperatives.

We look forward to partnering with governments to improve approaches to fostering trust while leveraging global data to strengthen cybersecurity and resiliency.



# **“Better Connected: How Cross-Border Data Flows Enable Stronger Cybersecurity”**



**CR2**  
COALITION TO REDUCE  
CYBER RISK