COUNTER RANSOMWARE INITIATIVE TABLETOP EXERCISE

AFTER-ACTION REPORT

GIGI FLORES BUSTAMANTE
ELIZABETH VISH

MARCH 2026

IST Institute for SECURITY + TECHNOLOGY

Counter Ransomware Initiative Tabletop Exercise: After-Action Report

March 2026

Authors: Gigi Flores Bustamante and Elizabeth Vish

Elizabeth Vish directs IST's global engagement on cyberspace issues. Before IST, she served in the U.S. Department of State's cyberspace policy team. She has a masters in International Relations with an emphasis on economics from Johns Hopkins School of Advanced International Studies.

Gigi Flores Bustamante is a Senior Associate at the Institute for Security and Technology, where she focuses on international public-private cyber initiatives. She holds an MA and a BA in Global Affairs from the Geneva Graduate Institute and Florida International University.

Design: Taylor White

IST

About the Institute for Security and Technology

Uniting technology and policy leaders to create actionable solutions to emerging security challenges

Technology has the potential to unlock greater knowledge, enhance our collective capabilities, and create new opportunities for growth and innovation. However, insecure, negligent, or exploitative technological advancements can threaten global security and stability. Anticipating these issues and guiding the development of trustworthy technology is essential to preserve what we all value.

The Institute for Security and Technology (IST), the 501(c)(3) critical action think tank, stands at the forefront of this imperative, uniting policymakers, technology experts, and industry leaders to identify and translate discourse into impact. We take collaborative action to advance national security and global stability through technology built on trust, guiding businesses and governments with hands-on expertise, in-depth analysis, and a global network.

We work across three analytical pillars: the **Future of Digital Security**, examining the systemic security risks of societal dependence on digital technologies; **Geopolitics of Technology**, anticipating the positive and negative security effects of emerging, disruptive technologies on the international balance of power, within states, and between governments and industries; and **Innovation and Catastrophic Risk**, providing deep technical and analytical expertise on technology-derived existential threats to society.

Learn more: https://securityandtechnology.org/

Acknowledgments

The Institute for Security and Technology (IST) wishes to thank the many individuals and organizations who contributed to the development and execution of this Counter Ransomware Initiative (CRI) public-private tabletop exercise. IST acknowledges the Government of Canada for funding this exercise through Public Safety Canada's Policy Development Contribution Program, as well as the Governments of Australia and the United Kingdom for their engagement and support. IST also thanks the leaders and members of the CRI Private Sector Advisory Panel for their participation, and the Government of Singapore for hosting the exercise on the margins of the 2025 Singapore International Cyber Week and the Fifth CRI Summit.

This exercise draws on materials developed for a ransomware tabletop exercise conducted by IST in partnership with Europol in 2024. That earlier exercise benefited from contributions from law enforcement and private sector representatives, including the Royal Canadian Mounted Police, the United Kingdom's National Crime Agency, and a global bank. IST thanks all of these contributors for their expertise and support, which helped inform the design of this exercise.

IST further thanks all participants in the CRI exercise for their time, engagement, and insights, which were essential to the discussions and findings reflected in this report.

Contents

Executive Summary

Ransomware remains a persistent and disruptive global threat to governments and the private sector. While public-private partnerships are widely recognized as essential to countering ransomware, both governments and private companies articulate serious gaps between desired levels of collaboration and the current real-world level of partnership. In this context, the Institute for Security and Technology (IST), in partnership with the Australian Department of Home Affairs and the Counter Ransomware Initiative (CRI) Private Sector Advisory Panel led by Public Safety Canada and BlackBerry, convened a multinational ransomware tabletop exercise (TTX) to examine how public and private stakeholders coordinate during a significant incident.

Held in October 2025 on the margins of Singapore International Cyber Week and the Fifth CRI Summit, the exercise brought together participants from various CRI member states and from the private sector for a multi-region, multistakeholder examination of the challenges facing public-private collaboration. Discussions focused on the operational realities and constraints that shape ransomware mitigation in practice, as well as the mechanisms that enable and challenge effective collaboration across jurisdictions.

Key Takeaways

The exercise generated valuable takeaways for strengthening international collaboration as well as information sharing:

- **Sharing information strategically can pay dividends.**

  Timely, targeted, and actionable information sharing between government and the private sector can improve incident preparedness and response coordination.

- **Victim-centric approaches can engender better outcomes.**

  Supportive government engagement—including clear guidance, trusted communication channels, and reduced fear of regulatory consequences—can encourage earlier incident reporting, expand response options for victims, and strengthen long-term public-private trust.

- **Coordination can help mitigate transnational friction.**

  Greater alignment on investigative priorities and stronger, ongoing dialogue on policy approaches can reduce conflicting guidance to victims and enable more effective multinational ransomware response and financial disruption efforts.

Background

Established in 2021, the Counter Ransomware Initiative (CRI) brings together governments and other key partners to strengthen international cooperation to combat ransomware.[1] Convened as a multilateral platform with governments and other entities as members, the CRI "builds collective resilience to ransomware, disrupts the ransomware ecosystem and designs policy approaches to combat ransomware."

To inform its work, the CRI engages with private sector stakeholders through the Private Sector Advisory Panel (PSAP), which serves as a mechanism for incorporating private sector perspectives into CRI discussions. The PSAP goals are: to facilitate collaboration between the public and private sector on ransomware; help CRI members to benefit from expertise from private sector entities; and build trust and foster proactive collaboration between the CRI and private, research, and non-profit entities.

The Institute for Security and Technology (IST) participates in the PSAP alongside other private sector organizations, including BlackBerry, Arctic Wolf, Ensign InfoSecurity, Microsoft, Palo Alto Networks,[2] and the Royal United Services Institute (RUSI). In this capacity, IST has contributed analytic input to CRI-related discussions and activities, including conducting prior work on public-private cooperation, information-sharing challenges, and ransomware defense practices.

Exercise Design

Overview and Objectives

The exercise was structured as a scenario-based tabletop exercise (TTX) designed to facilitate discussion among participants representing different roles across the counter-ransomware ecosystem. The overarching objectives of the exercise were to:

- Identify points where collaboration between CRI member states and the private sector could create friction for ransomware actors.
- Examine how information sharing related to financial transactions and ransomware actors' tactics, techniques, and procedures (TTPs) can support defensive, investigative, and disruption efforts.
- Explore policy and operational considerations that may facilitate more effective public-private collaboration to combat ransomware.
- Build trust among participants through in-person engagement and shared problem-solving.

1 For more information on the CRI, see the Initiative's website: https://counter-ransomware.org/.
2 Palo Alto Networks joined the PSAP in 2026.

The exercise emphasized exploratory discussion rather than evaluation, with the goal of surfacing practical challenges and insights across the global counter-ransomware landscape.

Scenario and Structure

The exercise scenario involved a fictional ransomware actor operating across multiple jurisdictions and targeting organizations through managed services providers and supply-chain relationships. The scenario built on the design of previous ransomware tabletop exercises conducted in 2024, and sought to examine questions relevant to the broad set of CRI members who were invited to participate, as well as the diverse sets of policy frameworks, legal landscapes, and technical approaches that encompass CRI members' national contexts.

» **Participants worked through the scenario in three phases:**

1. **Incident Reporting and Response:** Focusing on initial detections, victim engagements, and early information sharing
2. **Ransom Payment Consideration:** Examining payment-related decision-making and options for tracing or disrupting financial flows
3. **Post-Incident Response and Collaboration:** Exploring follow-on actions, cross-border coordination, and opportunities for longer-term disruption

Participation and Methodology

The exercise brought together representatives from approximately twenty government entities and ten private sector organizations. Participants were selected based on their ability to speak to institutional roles, authorities, and operational constraints, rather than to represent or role-play specific organizations. In contrast to previous exercises of this type that IST has convened, which have centered on a specific geographic region, contributors to this discussion included representatives from Africa, Europe, Asia, and the Pacific, spanning both middle and high income countries.

Over the course of the three and a half hour session, facilitators guided discussion through targeted injects, encouraging participants to describe their perspectives on information sharing, coordination, and prioritization at each stage of the scenario. Discussions were structured to encourage open and candid exchange among participants.

Phase 1: Initial Incident and Response

The exercise opened with a scenario involving ransomware incidents affecting several interconnected companies operating across multiple jurisdictions. Following the initial incident, the scenario reviewed processes that victims might initiate, including reporting to national

law enforcement and other government authorities relevant for combating ransomware. The scenario examined participants' views on the interactions between incident response firms and victims and questioned how law enforcement would engage the victim organization. Following initial reports from victim organizations, this phase examined how public and private stakeholders establish situational awareness and launch early response efforts.

Phase 2: Ransom Payment Consideration

In the second phase of the scenario, the simulated victim organization initiated the ransom payment process and notified government authorities, generating discussion on how law enforcement and private stakeholders engage once payment becomes a live consideration.

Participants first examined how government and private sector stakeholders interact with victims during ransom deliberations. Public sector participants described communicating official guidance, outlining risks, and discussing available options. Private sector participants noted that victims often weigh operational and business impacts alongside legal and reputational considerations when making decisions.

The discussion then turned to payment alternatives, including potential availability of decryption tools, technical mitigation strategies, and investigative options that may provide victims with additional pathways beyond paying the ransom. They also discussed how trusted networks and coordination mechanisms could facilitate rapid awareness of available technical support.

As the scenario progressed, the group examined issues related to payment transfer and financial tracing efforts. Private sector participants addressed reporting obligations and legal authorities. They noted that jurisdictions differ in their reporting frameworks and investigative capacities, which may influence how information flows and how quickly authorities can act.

Phase 3: Post-Incident Response and Infrastructure Disruption.

During the third phase of the exercise, the simulated threat actor transferred funds to a wallet associated with a service provider offering web hosting and related infrastructure. This development prompted discussion on how public and private stakeholders coordinate to identify, assess, and disrupt infrastructure that enables malicious activity. The scenario then turned to possibilities for longer-term collaboration against a specific threat actor, including coordination beyond incident response.

Thematic Analysis and Key Insights

Throughout the course of the discussions, the participants learned about the perspectives that different institutions bring to incident response and how each approaches questions of collaboration and information sharing. The exercise revealed several ways to strengthen counter-ransomware collaboration, including increased information sharing, adjustments to how governments engage with victims, and elimination of the points of friction that can hamper existing mechanisms for collaboration.

Theme One: Sharing information strategically can pay dividends

During the TTX, participants highlighted information sharing as a means to reduce vulnerabilities, support problem-solving, and facilitate coordinated action. Participants from both the private and public sectors raised questions about how to calibrate information sharing in fast-moving incidents. They weighed concerns about "flooding the zone" with low-priority or poorly contextualized information against the risk of withholding details that could be operationally relevant. The group acknowledged that governments and private network defenders will have complementary but distinct goals, and achieving those goals will benefit from clarity about what information is shared, with whom, and for what purpose.

PRIVATE SECTOR REPRESENTATIVES REQUESTED SHARING OF TECHNICAL INFORMATION FOR NETWORK DEFENSE

Private sector participants identified a clear gap between the information that governments share and the information that private sector defenders would like to receive. The private sector participants requested that governments share granular technical information to support defensive measures. Several noted that, when possible, they would benefit from high-level descriptions of victim targeting, along with more actionable details such as endpoint detection and response (EDR) data, indicators of compromise (IOCs), and clarity on initial access vectors. Private sector participants highlighted that timely sharing of this information with network defenders can prevent further compromise and additional attacks.

In a multinational context characterized by varying levels of cyber maturity and differing legal and operational authorities, these factors further amplify existing challenges and add complexity to cross-border coordination efforts, including the sharing of technical information or the solicitation of additional details from victims. Participants also recommended using existing national and international platforms to share threat assessments with partners, including the open-source protocol available through the Malware Information Sharing Platform (MISP). Not all CRI members or private entities will benefit equally from the same type

of information exchange. To make it more applicable, CRI members could start conversations on threat sharing by first clarifying what members want to do with the information. One area that CRI leaders could explore is creating an articulated set of recommendations on the type of priority information to share.

GOVERNMENT REQUESTS FOR INFORMATION FROM THE PRIVATE SECTOR CAN BE MORE STRATEGIC

Government representatives in the TTX articulated a desire to receive more strategic information from partners, most especially to receive timely information about TTPs and alerts regarding serious incidents; multiple governments noted that they would much prefer a rough initial report in a more timely manner rather than a finalized report from an entity once all information is collected and confirmed, which may take much longer. Governments also expressed a strong desire to build trust with the private sector in order to facilitate sharing information and asked what could be done to enhance this dialogue.

Private sector entities in the TTX articulated that governnts regularly request or even require victims to report or share information without articulating why the information is useful, how that information will be used, who will act on it, or if the sharing organization will hear back from the receiving government entity. Participants also noted that multiple governments often request the same information from victims following an incident—and some governments may even request that the same information be reported to multiple entities within a single government. As a result, organizations do not know how to prioritize their scarce employee time and energy and may default toward minimum compliance, limiting disclosure to what is strictly required. One government representative noted that their decision to encourage interim reporting of incidents as they develop had substantially improved the amount of useful information they receive from victims.

To reduce duplication and reporting fatigue, governments should work to align incident reporting channels and core reporting requirements. This alignment should look at several dimensions, including coordinating channels where victims report; articulating core information that should be reported; and setting clear expectations on timing so that victims understand what must be reported quickly versus what information can be shared at a later date. The goal in this process should not be to reduce overall information sharing, but rather to facilitate sharing of better, more timely information by articulating sequencing and providing consistency in requests. Private sector participants recommended that governments explain why they request that victims report specific types of information, including clearly delineating

what types of information are more time sensitive and what types of information are important for long-term investigation.

Alignment of incident reporting could substantially benefit both governments monitoring threats and the private sector entities responsible for responding to incidents and seeking to prevent further ransomware attacks. Governments can benefit by receiving information that is important in a timely manner.

Importantly, governments need to also address the question of how this information collection plays a long-term role in bolstering network defense at a national level. When more information is shared in a timely manner, network defenders throughout the ecosystem who can act quickly to prevent systems from being compromised stand to benefit.

The exercise reinforced that voluntary information sharing is most effective when stakeholders understand why information is being shared, who has the authority to act on it, and how it supports specific objectives. This suggests an opportunity for the counter-ransomware community to draw more deliberately on lessons from past efforts where information sharing led to tangible outcomes, such as successful disruption operations or asset recovery.[3] Clarifying what "successful" information sharing looks like in different operational contexts—and focusing on the elements that directly contribute to prevention, disruption, or recovery—could help ensure that future efforts are more purposeful, efficient, and outcome-oriented.

Theme Two: Victim-centric approaches can engender better outcomes

Participants highlighted that during an active incident, victims are often balancing business continuity, regulatory exposure, reputational risk, and legal uncertainty under highly compressed timelines. The way a government initially engages with an entity that may be experiencing a ransomware attack often sets the tone for the entire investigation, and can shape whether and to what extent a victim reports the contours of an incident, how much information they disclose, and which response options the victim considers viable. Victims, fueled by their desire to protect their reputation and any sensitive data and to reduce the likelihood that the criminal will continue to pursue their systems or that they will be victimized by another ransomware gang, may be incentivized to avoid extensive sharing of information. To increase the amount of information that governments receive from ransomware victims, government leaders should seek to create a culture where affected entities feel safe enough to work with them, supported by clear guidance, engagement with industry networks, and ongoing communication channels.

3 For research on successful examples of information sharing within the counter ransomware ecosystem, see: https://securityandtechnology.org/virtual-library/report/information-sharing-in-the-ransomware-payment-ecosystem/

Drawing on their experience working with victims, private sector participants encouraged governments to recognize that their approach can unintentionally overwhelm organizations already in the throes of coping with a crisis. Governments' regulatory authority and enforcement powers may cause information requests to be perceived as high-stakes compliance obligations rather than supportive engagement. Effectively engaging with victims requires recognizing that, for a CISO in the thick of an ongoing incident, this could very well be their "worst day ever." Practically speaking, offering safe harbor so that information shared voluntarily does not lead to more severe fines or other non-monetary regulatory repercussions could substantially help to open lines of communication. An example of this type of arrangement includes the U.S. Cybersecurity Information Sharing Act of 2015.

Private sector participants further expressed how law enforcement engagement can shape the options available to victims considering payment. Several noted that, in some jurisdictions, law enforcement may have the capacity to trace ransom payments or support disruption efforts, potentially influencing how victims evaluate payment as a response option. Law enforcement agencies and other entities also have access to decryptors, but victims are not always aware of these, leaving them unable to seek that option.

In addition to changing how law enforcement approaches victims after they experience a ransomware attack, the discussion highlighted that creating a culture of safe reporting to the government requires an ongoing effort by cybersecurity authorities to build rapport with the broader ecosystem of actors that victims are most likely to turn to first. This includes sectoral networks, cyber insurers, digital forensics and incident response (DFIR) firms, and managed service providers. These stakeholders often serve as trusted intermediaries between victims and government authorities.

Strengthening relationships with this ecosystem can improve the timeliness and quality of incident reporting, facilitate information sharing, and enable more coordinated responses to ransomware threats. Public and private sector stakeholders should therefore view victim engagement as an integral part of their broader counter-ransomware strategy. This includes creating and publicizing pathways where victims can turn to trusted points of contact for assistance.

Integrating these relationships into routine engagement and preparedness efforts can ultimately support long-term cooperation. However, this will only work if victims—and their points of contact—find that they receive assistance, rather than face punishment, when they engage government partners.

Theme Three: Coordination can help mitigate transnational friction

With a diverse set of jurisdictions and multinational companies participating, the exercise also identified areas where lack of coordination between different actors has reduced the effectiveness of counter-ransomware efforts.

LAW ENFORCEMENT ENTITIES FROM DIFFERENT COUNTRIES SOMETIMES GIVE VICTIMS CONFLICTING DIRECTIONS

During the multinational scenario, participants highlighted the challenges that arise when different governments take divergent approaches to the same threat actor. Given that ransomware incidents may take place in multinational companies with subsidiaries in multiple national jurisdictions, this can present serious complications for victims. For example, one government may tacitly permit a victim to pay and work with that victim to track that money for intelligence purposes; at the same time, another government may tell a victim to cut off the engagement with the criminal and not to pay a ransom given ongoing sanctions or other concerns.

While different governments will likely continue to have different approaches, especially given the overall geopolitical context, the Counter Ransomware Initiative could serve as an additional forum for law enforcement stakeholders to discuss ransomware-specific priorities, share approaches, and reduce friction across jurisdictions. Given the CRI's unique nature as a trans-region, voluntary effort, this could complement existing operational cooperation mechanisms such as Europol and INTERPOL.

AVOIDING PAYING IS CHALLENGING, BUT THERE ARE OPPORTUNITIES TO MAKE DOING SO EASIER

Participants framed payment decisions as occurring under real-world constraints. They emphasized that deciding not to pay demands significant time, coordination, and resources. Even if companies are not able to immediately decide not to pay, industry participants voiced that there may be a spectrum of approaches, including opportunities to slow negotiations with threat actors in order to better analyze options or put in place counter measures.

The discussion also surfaced challenges related to coordination and dissemination of decryptors. Participants questioned whether decryptor availability and similar capabilities should flow through centralized platforms, trusted peer networks, or ad hoc "call for help" mechanisms, and the discussion did not produce consensus around any single model. Several emphasized that lack of awareness of decryptors and difficulties in accessing them may limit the effectiveness of these options, even when technical solutions exist.

COORDINATION CAN CUT A RANSOMWARE CRIMINAL'S "PAYOUT"

Anti-money laundering efforts can substantially reduce the profitability of ransomware crimes, but cryptocurrency's ability to intersect with multiple different national financial systems makes anti-money laundering efforts more challenging by complicating jurisdictional oversight, slowing coordination among regulators, and enabling funds to be transferred or converted across borders quickly. Different jurisdictions have different standards for seizures of funds. One new development in countering money laundering is the Silver Notice that was piloted by INTERPOL in 2025. This effort, described on INTERPOL's website, offers a way for jurisdictions to request the seizure or freeze of funds held by exchanges headquartered in other INTERPOL member states.

Conclusion

Exercises like the one conducted in Singapore on the sidelines of the Fifth Counter Ransomware Initiative Summit can create space to surface points of friction and ask difficult questions in a low-risk environment. Conflicting priorities, capacity limits, and uncertainty around roles or authorities present real challenges to governments and private sector entities trying to collaborate to reduce the harm caused by an incident—but these circumstances are also often the conditions under which collaboration actually takes place.

In building public-private partnerships and articulating practices for public-private engagement, governments and private partners should treat these constraints as a core design assumption, not as a secondary challenge. By acknowledging capacity limits upfront, stakeholders can design collaboration models that prioritize the most effective actions first. Designing response mechanisms and disruption efforts that function under constrained conditions may enable more proactive and coordinated action during incidents, even when partners cannot engage at full scale.

Despite the substantial challenges articulated in this report, partners in the TTX were adamant that they wanted to actively collaborate to take down ransomware hackers and cut off their profits. Private sector partners in the exercise repeatedly highlighted their desire to work with law enforcement, and expressed in particular a willingness to go beyond information sharing into active disruption and collaboration to stop ransomware attacks from happening. As the CRI continues to develop project priorities, the TTX made it clear that there is an opportunity to join forces with private sector partners in order to tackle real challenges.

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org