FOR IMMEDIATE REPORTING

CRI STEERING COMMITTEE SUMMARY FOR 2025

Our Shared Vision and Commitment

At the meeting of the 5th International Counter Ransomware Summit (CRI) in Singapore on 24 October 2025, 74 members of the CRI reaffirm our joint commitment to:

- Build collective resilience to ransomware and support members facing attacks including learning from each other on policy and operational response
- Hold criminal ransomware actors and their enablers to account and deny them safe haven
- Counter the use of enablers that underpin the ransomware business model.
- Forge robust international partnerships and work closely with the private sector as allies
- Encourage active information sharing among members to build trust and facilitate knowledge exchange
- Promote responsible state behaviour in cyberspace, identify criminal ransomware actors and call out their acts wherever they occur

Key Pillars of Action in 2025

The International Counter Ransomware Task Force (ICRTF), co-led by Australia and Lithuania, continued to uplift operationally focused information sharing between members and promote efforts to disrupt ransomware criminals. The ICRTF sought to amplify real-time responses to ransomware and highlighted case studies to better prepare member countries and non-government members. This included a series of virtual workshops focused on the cybersecurity of critical infrastructure, and the cyber threats posed by ransomware actors.

The CRI adopted the *CRI Information Sharing Governance Framework,* which was developed by the ICRTF's Information Sharing Working Group and sought to answer the key questions of: *where, when, how and with whom* information should be shared in the CRI. This framework should serve as the primary guideline for CRI members to share information and enhance awareness of ransomware threats posed by ransomware actors. The Framework was presented at the CRI Summit and endorsed by the membership.

Australia continued to manage the CRI website and members' portal, and is growing the catalogue of alerts, resources and contacts available to members. Since its inception in 2023, the public website has received more than 2.1 million hits while the members' portal has been accessed more than 100,000 times. Since the last CRI Summit, five member countries utilised the portal to seek assistance from other members to counter ransomware attacks.

In collaboration with the Public-Private Sector Advisory Panel (PSAP), the ICRTF is exploring opportunities to create an enhanced incident response assistance mechanism to assist members in the event of a ransomware attack. An improved web portal and

assistance mechanism will enhance the cyber resilience of CRI members and reduce the impact from high severity ransomware incidents.

The PSAP, in collaboration with the ICRTF and led by private sector partners, Institute for Security and Technology (IST) and BlackBerry, delivered a tabletop exercise with CRI members on coordinated responses to significant ransomware attacks. Members identified opportunities for international and public-private coordination to address and resolve threats, counter the use of virtual assets in illicit activities like ransomware, and to bring criminal ransomware actors to account.

The PSAP collaborated with CRI members to develop two papers on the global cybersecurity environment. The first, the Ransomware Trends and Reporting Technical Paper, explores emerging trends and themes in ransomware related activity from the perspective of cybersecurity and law enforcement agencies across the world. The Bulletproof Hosting paper explores the role of cloud and hosting providers that shelter fraudulent customers. The relationship between bulletproof hosting and cybercrime is explored, and guidance is given on mitigating the risks.

Noting the importance of engagement between government and the private sector, the PSAP and the Private Sector Engagement Working Group have also developed guidance for the CRI membership on public-private sector partnerships. This includes a Protocol for Engagement that will help inform how governments can effectively engage private sector entities.

The Policy Pillar, co-led by the United Kingdom and Singapore, has continued to drive efforts to share best practices on developing policies to enhance resilience and influence victim behaviour to mitigate the impact of and reduce the rising global ransomware threat.

This year, the United Kingdom and Singapore have developed a Supply Chain Guidance, endorsed by 67 CRI members. As supply chains are often a key point of vulnerability for many organisations, the guidance document provides specific recommendations that organisations should be looking out for in their supply chains. The guidance aims to highlight the risks of ransomware to organisations and their supply chains, as well as promote good cyber hygiene to protect supply chains. Vulnerabilities in modern complex supply chains can inadvertently provide an entry point for threat actors to execute a ransomware attack. This guidance seeks to address the supply chain risks, including in the procurement process, by ensuring that CRI members and wider organisations heed expert and evidence-driven advice to improve their supply chain security posture.

Additionally, Portugal has led a project that measures the impact on the 2024 CRI Guidance for Organisations developed with the insurance industry. The report evaluates the effectiveness of its dissemination of the 2024 guidance, identifying how the product has been adopted by government agencies and insurance bodies and where it has been most effective during incident response.

The European Union and Singapore have led a project on Securing our Internet of Things (IoT) against ransomware actors. This project has focused on understanding how vulnerabilities in IoT devices can be exploited for ransomware attacks and seeks to mitigate the risks. The European Union and Singapore have completed an evidence-gathering exercise, analysed its findings and, developed key policy recommendations that members can adopt to enhance resilience of IoT devices.

The Republic of Korea has led a project that looks at Best Practices for Ransomware Legislation. This project identifies and maps national legislative measures countering ransomware and assesses the effectiveness and limitations of these measures. The proposed ransomware legislative measures by the United Kingdom, which were the focus of public consultation in 2025, and by Italy, currently under discussion in Parliament, are key areas that CRI members could learn from.

In addition to these projects, the Policy Pillar hosted virtual tabletop exercises, simulating an escalating ransomware crisis targeting the health sector. The goal was to encourage collaboration between CRI members and build greater awareness of the policy standpoints of the CRI during stages of incident response, with 35 participating members.

The Diplomacy and Capacity Building (DCB) Pillar, co-led by Germany and Nigeria, expanded the CRI's partnerships by welcoming Armenia, Chile, Cyprus, Latvia, Saudi Arabia and the World Bank to the coalition. The DCB pillar developed guidelines on hosting side events in order to facilitate CRI member-led regional activities and workshops.

In collaboration with private sector partners of the PSAP, the IST and Ensign InfoSecurity, the DCB Pillar delivered a workshop on building Public-Private Partnerships (PPPs) to mitigate ransomware. The workshop convened CRI member and private sector partners to explore best practices on setting up PPPs, including IST's six-step framework for Initiating PPPs that are reflected in the aforementioned CRI's Protocol for Engagement on PPP. In collaboration with Germany, the private sector partner Royal United Services Institute (RUSI) is currently undertaking a project to develop a practical framework to help CRI members assess the effectiveness of different ransomware countermeasures.

Looking Ahead

Over the past five years, we have forged a powerful coalition of partners, united by a common purpose. But despite our best efforts, we are failing to deter or degrade ransomware actors and the dark ecosystem they operate within. The threat is evolving—and so must we.

All CRI members will continue to strengthen the resilience of participating states, drive real and measurable progress, and ensure that our strategies evolve as rapidly as the threat itself. Together, we will move from words to action—delivering tangible results for a safer, more resilient digital future.