RANSOMWARE TASK FORCE

# DOUBLING DOWN

## APRIL 2024 PROGRESS REPORT

IST Institute for SECURITY + TECHNOLOGY

# THE RANSOMWARE TASK FORCE: DOUBLING DOWN

RANSOMWARE
TASK FORCE

April 2024

# Contents

# 2023-2024 Milestones

Key: Policy | Resource | Disruption/Sanction | Awareness

**March 1, 2023** With the launch of the National Cybersecurity Strategy, ransomware is underscored as a national security threat.

**March 23, 2023** CISA launches the Pre-Ransomware Notification Initiative.

**July 13, 2023** The White House publishes the National Cybersecurity Strategy Implementation Plan.

**September 2023** CISA releases ransomware tabletop exercise materials.

**September 19, 2023** DHS publishes harmonization of ransomware reporting recommendations.

**October 26, 2023** Additional countries sign on to an update to the April 2023 secure-by-design guidance, bringing the total to 17 countries.

**March 13, 2023** CISA launches the Ransomware Vulnerability Pilot program (RVWP).

**April 13, 2023** The United States, Australia, Canada, the UK, Germany, and the Netherlands publish secure-by-design guidance.

**July 26, 2023** The U.S. Securities and Exchange Commission (SEC) announces new ransom disclosure rules.

**August 29, 2023** An international cyber takedown effort disrupts Qakbot malware infrastructure.

**October 2023** CISA expands the Ransomware Vulnerability Warning Pilot program (RVWP).

**October 2023** International police coordination disrupts the Ragnar Locker ransomware gang.

# Tracking Progress Against Ransomware

A non-exhaustive list of policy actions, newly-published resources, moves to disrupt or sanction ransomware actors, and efforts to bring awareness to the threat.

**November 3, 2023** CISA launches "Shields Ready" campaign for critical infrastructure.

**November 2023** The U.S. Treasury Department sanctions a Russian actor accused of laundering virtual currency on behalf of an affiliate of the Ryuk ransomware group.

**November 1, 2023** CRI members endorse the first-ever joint CRI policy statement declaring that member governments should not pay ransoms.

**November 21, 2023** EUROPOL works with seven other countries to dismantle a ransomware group operating in Ukraine, leading to several arrests and detentions.

**December 2023** New York Department of Financial Services announces new ransom disclosure rules.

**December 2023** The U.S. Justice Department, with European law enforcement support, disrupts ALPHV/Blackcat ransomware variant.

**January 2024** GAO releases report urging agencies to enhance oversight of ransomware practices and better assess federal support.

**January 19, 2024** OFAC Senior Compliance Officer reiterates commitment to clarifying ransom payment guidance.

**January 2024** Australia, the United Kingdom, and the United States issue the first trilateral sanctions designating a Russian cyber actor involved in a 2022 ransomware attack in Australia.

**February 5, 2024** ODNI releases annual threat assessment, naming ransomware as a transnational threat to the United States.

**February 26, 2024** NIST publishes Cybersecurity Framework 2.0.

**February 20, 2024** The United States and the UK, along with international law enforcement partners, announce the takedown of LockBit ransomware variant.

**February 20, 2024** The U.S. Treasury Department sanctions affiliates of the LockBit ransomware group.

**March 27, 2024** The U.S. Department of State's Rewards for Justice Program announces a reward for ALPHV/Blackcat-linked cyber actors.

**March 20, 2024** DHS and DG CONNECT announce initiative to compare cyber incident reporting and better align transatlantic approaches.

**April 4, 2024** CISA publishes Notice of Proposed Rulemaking for CIRCIA.

# Executive Summary

In April 2021, the Ransomware Task Force (RTF) published *Combating Ransomware: A Comprehensive Framework for Action* ("the Report"), which outlined 48 recommendations for industry, government, and civil society to undertake in order to **deter** and **disrupt** the ransomware ecosystem, and to help entities **prepare** for and **respond** to attacks at scale.[1] In the three years since its publication, we have continued to see governments and the private sector step up commitments to addressing this threat. However, ransomware remains a major national security threat based on its cost to the economy and impact on critical services availability. The rate and scale of attacks is not diminishing and may be growing. For the first time ever, Chainalysis reported that ransomware payments had surpassed $1 billion in 2023.[2]

Since our May 2023 progress report, the U.S. government and its partners have intensified disruption efforts, increased information sharing, and developed more comprehensive ransomware mitigation and recovery strategies. However, of the 48 recommendations made in the Report, our assessment remains unchanged: only 24 have seen significant progress since the Report's release in 2021.

IST's view is that the 48 original recommendations remain relevant and important to implement to reduce the threat that ransomware poses to the United States and the global digital ecosystem. Given this assessment, this progress report focuses on the 24 recommendations that have seen little to no action since 2021, identifying how governments and industry can achieve substantial results by doubling down on these key Report recommendations.

As noted in previous progress reports, these 24 recommendations are more difficult to implement; in the United States, many would require legislative action.[3] While governments deserve praise for the mechanisms they have put in place, our assessment is that the United States is not using them to their full extent. First, the United States and other governments have not yet allocated sufficient resources to these existing mechanisms. Second, governments have not taken all necessary further actions to combat ransomware. The Ransomware Task Force remains committed to engaging with the United States and like-minded governments, industry partners, and civil society to raise awareness and advocate for effective solutions to mitigate the dangers of ransomware.

This progress report identifies areas in need of sustained action, as well as areas in need of new or heightened progress, ultimately aiming to double down on the Ransomware Task Force recommendations.

1 "Combating Ransomware: A Comprehensive Framework for Action," Institute for Security and Technology, April 30, 2021, https://securityandtechnology.org/ransomwaretaskforce/report/.

2 "Ransomware Payments Exceed $1 Billion in 2023, Hitting Record High After 2022 Decline," Chainalysis, February 29, 2024, https://www.chainalysis.com/blog/ransomware-2024/.

3 "The Ransomware Task Force: One Year On," Institute for Security and Technology, May 2022, https://securityandtechnology.org/wp-content/uploads/2022/05/rtf-progress-report-may22-1.pdf; "The Ransomware Task Force: Gaining Ground," Institute for Security and Technology, May 2023, https://securityandtechnology.org/wp-content/uploads/2023/05/Ransomware-Task-Force-Gaining-Ground-May-2023-Progress-Report.pdf.

- A number of areas have seen sustained action by governments, but they must capitalize on the opportunities they already have in place in order to make substantive progress, including through leveraging existing legislation and allocating additional resources to combat the ransomware threat.
    - **Harmonizing Incident Reporting Mechanisms:** Much headway has been made to improve incident reporting structures. The United States and other partner countries still need to capitalize on current opportunities for streamlining incident reporting in order to lessen the burden on victims and increase the efficacy of response activity.
    - **Expanding International Collaboration:** Global collaboration continues to grow, despite significant outlier governments that are unwilling to take action against ransomware actors operating from their territory. Governments should continue to work together to share information and step up deterrence and disruption efforts.
    - **Reining in Ransom Payments:** As debates around payment bans continue, governments need to take concrete steps to make ransomware less profitable for bad actors and less devastating for victims.
- Meanwhile, in other areas that have seen little to no action, governments, civil society, and industry need to initiate new or redoubled efforts.
    - **Disrupting Ransomware At Scale:** Coordinated law enforcement and private sector interventions are successfully disrupting ransomware operations, but need to be performed at scale for effective, long-term impact.
    - **Fostering Public-Private Partnerships:** Governments cannot go it alone, and need to lean on industry and other partners to foster a more resilient ecosystem.
    - **Bolstering Resilience and Building Awareness:** Organizations that follow best practice cybersecurity guidance provided by NIST, CISA, and related organizations (both in the United States and in other jurisdictions) have been able to dramatically increase their business resilience. Governments need to increase whole-of-nation awareness of these best practices and continue to make these resources easily accessible.
    - **Committing Financial Resources for Preparation and Response:** The United States and like-minded countries need to further invest in supportive measures for critical infrastructure and SMEs to prepare for attacks and respond effectively.

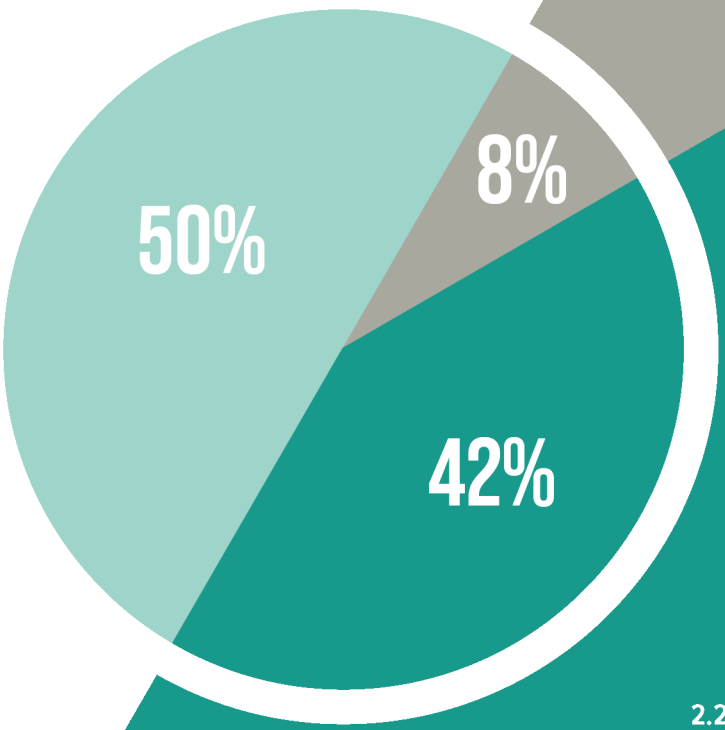
Before detailing our findings below, we want to note that as far as possible, the RTF tracks government responses to ransomware around the world. To date, the U.S. government has typically been among the most transparent and communicative about steps being considered or taken to combat ransomware. This is partly cultural, but may also reflect that, according to reporting data, the United States is still the most attacked nation,[4] and its economy experiences the greatest losses.[5] As such, while we have attempted to incorporate geographically varied and relevant data and examples in our reporting, our primary focus is on the actions and impacts of the U.S. government and in the United States.

4 Silas Cutler, "2022 RTF Global Ransomware Incident Map: Attacks continue worldwide, groups splinter, education sector hit hard," Institute for Security and Technology, October 31, 2023, https://securityandtechnology.org/blog/2022-global-ransomware-incident-map/.

5 "The 471 Cyber Threat Report 2023," Intel471, August 7, 2023, https://intel471.com/resources/whitepapers/the-471-cyber-threat-report-2023; Zeba Siddiqui, "Alliance of 40 Countries to Vow Not to Pay Ransom to Cybercriminals, US Says," *Reuters*, October 31, 2023, https://www.reuters.com/technology/alliance-40-countries-vow-not-pay-ransom-cybercriminals-us-says-2023-10-31/; Shmuel Gihon, "Ransomware Trends 2023 Report," Cyberint, April 8, 2024, https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report/.

# Ransomware Task Force Recommendations: April 2024 Status

| | |
|---|---|
| Significant Action | **24** |
| Preliminary Action | **20** |
| No Known Action | **4** |




## NO KNOWN PROGRESS

### Disrupt

**2.2.2**: Clarify lawful defensive measures that private-sector actors can take when countering ransomware.

### Respond

**4.3.1**: Require organizations to review alternatives before making payments.
**4.3.2**: Require organizations to conduct a cost-benefit assessment prior to making a ransom payment.
**4.3.3**: Develop a standard cost-benefit analysis matrix.

## SOME KNOWN PROGRESS

### Deter

**1.1.3**: Create a global network of ransomware investigation hubs.
**1.2.3**: Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign.

### Disrupt

**2.1.1**: Develop new levers for voluntary sharing of cryptocurrency payment indicators.
**2.1.3**: Incentivize voluntary information sharing between cryptocurrency entities and law enforcement.
**2.1.5**: Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation.
**2.1.7**: Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.
**2.2.1**: Leverage the global network of ransomware investigation hubs.
**2.3.2**: Create target decks of ransomware developers, criminal affiliates, and ransomware variants.

### Prepare

**3.1.3**: Highlight available Internet resources to decrease confusion and complexity.
**3.2.2**: Run nationwide, government- backed awareness campaigns and tabletop exercises.
**3.3.2**: Require local governments to adopt limited baseline security measures.
**3.3.3**: Require managed service providers to adopt and provide baseline security measures.
**3.4.4**: Alleviate fines for critical infrastructure entities that align with the Ransomware Framework.
**3.4.5**: Investigate tax breaks as an incentive for organizations to adopt secure IT services.

### Respond

**4.1.1**: Create ransomware emergency response authorities.
**4.1.3**: Increase government resources available to help the private sector respond to ransomware attacks.
**4.1.4**: Clarify United States Treasury guidance regarding ransomware payments.
**4.2.2**: Create a standard format for ransomware incident reporting.
**4.2.3**: Encourage organizations to report ransomware incidents.
**4.2.4**: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment.

# Introduction: The Evolving Threat Landscape

Ransomware incidents continue to impact organizations in every sector of the economy, especially critical sectors like healthcare, transportation, and education, including smaller, under-resourced entities. The FBI's IC3 reported an 18% increase in ransomware incidents from 2022, with adjusted losses of almost $60 million. The IC3 also noted that they received 1,193 reports of a ransomware incident from critical infrastructure organizations, a 37% increase from the 870 reports it received in 2022.[6]

Even as the number of reported incidents is on the rise, the FBI IC3 report also noted that many ransomware events continue to go unreported, greatly limiting cybersecurity and law enforcement communities' understanding of the frequency and disruption of ransomware incidents, not just in the United States, but also worldwide. Organizations throughout the cyber response ecosystem—including law enforcement, insurers, incident responders, cryptocurrency analysis firms, and others—track and analyze as much data as they are able to access, with the goal of reporting new patterns of criminal activity, including evolving tactics, techniques, and procedures (TTPs), and providing a sense of costs of recovery and ransom payment trends. The RTF reviews as many of these sources as possible to help inform our evaluation of the effectiveness of activities undertaken to address the ransomware threat and the impact of these actions.

In 2023, ransomware groups increasingly used multiple variants against a single organization and employed new data-destruction tactics to further pressure organizations into paying.[7] Many actors are also shifting away from encryption and into data exfiltration and exposure in order to gain more traction against organizations who have sufficient backups.[8] For example, a July 2023 Sophos report found that 25% of attacks against the financial sector included both data encryption and data exfiltration.[9]

As some potential victims have bolstered organizational preparedness for a potential attack, 2023 saw threat actors becoming more creative and aggressive in their pursuits. Threat actors intensified behavior, focusing their efforts against high-profile organizations and critical infrastructure. Ransomware actors have also turned toward zero-day exploits to target widely-used IT services

6 "Federal Bureau of Investigation Internet Crime Report 2022," FBI Internet Crime Complaint Center, March 10, 2023, 14, https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf; "Federal Bureau of Investigation Internet Crime Report 2022," 13.

7 "Federal Bureau of Investigation Internet Crime Report 2023," 3.

8 "Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days," Akamai Technologies, August 7, 2023, https://www.akamai.com/resources/state-of-the-internet/ransomware-on-the-move.

9 Sophos, "The State of Ransomware in Financial Services 2023," July 2023, https://assets.sophos.com/X24WTUEQ/at/skqcw8qv736cwr5hmtkxfwg/sophos-state-of-ransomware-financial-services-2023-wp.pdf.

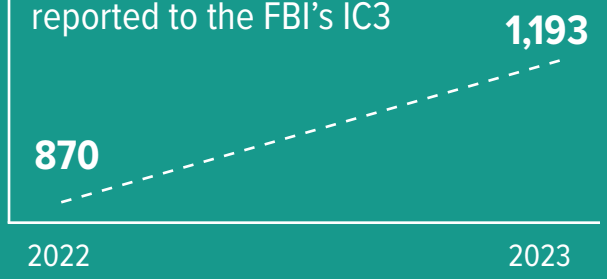
## KEY RANSOMWARE STATISTICS: 2023

**$1 billion**

in cryptocurrency extorted from victims of ransomware attacks, per Chainalysis

**37% increase in ransomware attacks on critical infrastructure**

reported to the FBI's IC3




**↑ 18% increase**

in ransomware attacks reported to the FBI's Internet Crime Complaint Center (IC3) from 2022 to 2023

According to Sophos, 25% of attacks against the financial sector **included both data encryption and data exfiltration**

In 2023, according to Google, four ransomware actors exploited

**6 zero-day vulnerabilities**

like MOVEit and GoAnywhere file-transfer services, Citrix networking products, and PaperCut print management software.[10] Google reported that four threat actors used six different zero days in ransomware attacks.[11] CL0P, a group active since at least 2019, appears to be one of the major pioneers leveraging zero days in its ransomware attacks.[12] Akamai Technologies, a cloud company, cited the use of zero- and n-day vulnerabilities as a key factor in the rise of ransomware attacks.[13]

Ransomware groups face economic trade-offs in deciding whether to exploit zero-day vulnerabilities, which can be costly to obtain and lose much of their value the first time they are used. The fact that any groups have used zero-days to both intimidate victims and wreak extreme harm signals that ransomware will remain a threat even though resilience is increasing. This tactic is one to watch and forthcoming reporting requirements should help assess whether it was a temporary shift or a new, troubling, trend.

Some threat actors have also begun to focus on more sophisticated social engineering attacks, such as targeting internal IT help desks. A consortium of actors often known as Scattered Spider has been known to employ such techniques, leveraging native English speaking capabilities to trick users into

10 Jai Vijayan, "Ransomware Victims Surge as Threat Actors Pivot to Zero-Day Exploits," DarkReading, December 8, 2023, https://www.darkreading.com/threat-intelligence/ransomware-victims-surge-as-threat-actors-pivot-to-zero-day-exploits; Matt Kapko, "Ransomware Actors Hit Zero-Day Exploits Hard in 2023," *Cybersecurity Dive*, February 8, 2024, https://www.cybersecuritydive.com/news/ransomware-surge-zero-day-exploits/706983/.

11 James Sadowski and Maddie Stone, "A Review of Zero-Day In-The-Wild Exploits in 2023," Google (blog), April 5, 2024, https://blog.google/technology/safety-security/a-review-of-zero-day-in-the-wild-exploits-in-2023/.

12 Shunichi Imano and James Slaughter, "Ransomware Roundup - Cl0p | FortiGuard Labs," Fortinet (blog), July 21, 2023, accessed April 16, 2024, https://www.fortinet.com/blog/threat-research/ransomware-roundup-cl0p#:~:text=The%20Cl0p%20ransomware%20has%20been%20around%20since%20early%202019%2C%20and,active%20ransomware%20threat%20actors%20today.

13 "A Year in Review: A Look at 2023's Cyber Trends and What's to Come," Akamai Technologies, November 14, 2023, https://www.akamai.com/lp/soti/2023-year-review.

handing over key credentials.[14] The U.S. Cybersecurity and Infrastructure Agency (CISA) has publicized these tactics, warning of their growing sophistication.[15]

However, most ransomware groups continue to operate using fairly unsophisticated attack methods. At present, the majority of organizations are still largely unprepared for even common cyber attacks, and cyber criminals do not typically need to use more complex or expensive approaches when well-crafted phishing emails remain largely effective.[16]

Speculation is rife on how ransomware groups will capitalize on the use of AI. Much has been written about the anticipated use of the technology to refine phishing communications to gain access to victim systems.[17] This type of activity would likely be undertaken by less sophisticated hackers using mass-market AI chat bots. However, AI-based attacks could be viable in the context of a growing number of mobile devices and internet-of-things (IoT), which often have poorer security features and create new avenues for potential attack.[18] 5G technology, if not managed effectively, will also bring more devices online without adequate security, making them easy targets for ransomware.[19] Other organizations have warned that criminals may leverage the technology to develop more automated, hard-to-detect, or sophisticated attacks.[20] AI has also made deep fakes—particularly voice-based deep fakes—cheaper to produce and deploy, creating new opportunities for phishing attacks.[21] More sophisticated and bespoke AI applications for extortion attacks will likely take much longer to emerge, and attackers may only invest in this activity as and when it becomes necessary.

On a positive note, AI also provides new opportunities for cyber defensive measures that should not be overlooked. Advancements in machine learning (ML) could be used to help bolster cyber defenses, particularly if they are used to strengthen resilience by creating system diversity and redundancy. ML innovation needs to be undertaken carefully and thoughtfully, with security-by-design at the forefront.[22]

---

14 Bill Toulas, "FBI Shares Tactics of Notorious Scattered Spider Hacker Collective," *BleepingComputer*, November 17, 2023, https://www.bleepingcomputer.com/news/security/fbi-shares-tactics-of-notorious-scattered-spider-hacker-collective/#google_vignette; Kristopher Russo, Austin Dever, and Amer Elsad, "Threat Group Assessment: Muddled Libra (Updated)," Palo Alto Networks Unit 42, March 8, 2024, https://unit42.paloaltonetworks.com/muddled-libra/.

15 "Scattered Spider," Cybersecurity and Infrastructure Security Agency, November 16, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a.

16 UK Home Office Department for Science, Innovation, and Technology, "Official Statistics: Cyber security breaches survey 2024," April 9, 2024, 7, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2024/cyber-security-breaches-survey-2024; "2024 SonicWall Cyber Threat Report," SonicWall, February 21, 2024, https://www.sonicwall.com/medialibrary/en/white-paper/2024-cyber-threat-report.pdf; "Phishing Threat Trends Report," Egress, October 2023, https://www.egress.com/media/mq4kwitu/egress_phishing_threat_trends_report.pdf; Bob Violino, "AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails, *CNBC*, November 28, 2023, https://www.cnbc.com/2023/11/28/ai-like-chatgpt-is-creating-huge-increase-in-malicious-phishing-email.html; Puja Mahendru, "The State of Ransomware in Financial Services 2023," Sophos News, July 10, 2023, https://news.sophos.com/en-us/2023/07/13/the-state-of-ransomware-in-financial-services-2023/.

17 Maya Horowitz, "Introduction to the 2024 Cyber Security Report," Check Point, February 21, 2024, https://go.checkpoint.com/2024-cyber-security-report/chapter-01.php.

18 Scott Sayce, "3 trends set to drive cyberattacks and ransomware in 2024," World Economic Forum, February 22, 2024, https://www.weforum.org/agenda/2024/02/3-trends-ransomware-2024/#:~:text=Cybersecurity,-Follow&text=Ransomware%20attacks%20saw%20a%20sharp,breaches%20up%20to%20a%20thousandfold.

19 Sayce, "3 trends set to drive cyberattacks and ransomware in 2024."

20 "The near-term impact of AI on the cyber threat," UK National Cyber Security Centre, January 24, 2024, https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat.

21 Margi Murphy, "The Next Wave of Scams Will Be Deepfake Video Calls From Your Boss," *Bloomberg*, August 25, 2023, https://www.bloomberg.com/news/articles/2023-08-25/deepfake-video-phone-calls-could-be-a-dangerous-ai-powered-scam?leadSource=uverify%20wall&embedded-checkout=true.

22 Wyatt Hoffman, "Making AI Work for Cyber Defense," Center for Security and Emerging Technology, December 2021, https://cset.georgetown.edu/publication/making-ai-work-for-cyber-defense/.

# Actions Requiring Sustained Effort

As noted above, the United States and governments worldwide have taken major steps toward putting policies in place to help reduce the national security threat posed by ransomware. Previous RTF progress reports have noted in particular that the U.S. Congress and the Executive Branch were quick to act after several major ransomware incidents in 2021 (e.g., Colonial Pipeline, Irish Health Services, and JBS meat processing) raised the profile of the problem.[23] We applaud these efforts; however, there are still several critical areas requiring continued or increased action.

## Harmonizing Incident Reporting Mechanisms

IST and the Cyber Threat Alliance published a Cyber Incident Reporting Framework in November 2022 that outlined the many benefits of creating a standardized, easily accessible reporting mechanism, including enabling better trend identification and facilitating information sharing among the U.S. government and partner countries **(Action 4.2.2)**.[24] However, proliferating reporting requirements are in fact using idiosyncratic templates that vary widely between jurisdictions—even varying widely within the same jurisdiction between multiple overlapping receiving agencies. Information sharing between reporting venues continues to be largely voluntary and ad hoc.

Increasing reporting of ransomware and other significant cyber incidents has been a key priority area for the United States and other like-minded governments. The passage of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) is just one prominent example of efforts to mandate and streamline incident reporting. However, there remains room for further progress to harmonize this work globally.

CIRCIA—which was signed into law on March 22, 2022—gave CISA a two-year period to draft a notice of proposed rulemaking (NPRM). Once in place, these reporting mechanisms should facilitate better insights into critical infrastructure vulnerabilities, trends in threats and cybercrime tactics, and incident preparedness. The NPRM, which was officially published on April 4, 2024, provides for an additional 18 months of internal government review and adjudication before it goes into effect in the fall of 2025. The public, however, only has two months—until June 2024—to submit comments before CISA begins working on the final reporting structure. IST, alongside industry and civil society groups, signed a letter

23 "The Ransomware Task Force: One Year On," 5.

24 "Cyber Incident Reporting Framework," Institute for Security and Technology, Cyber Threat Alliance, and industry organizations, November 2022, https://securityandtechnology.org/wp-content/uploads/2022/11/Cyber-Incident-Reporting-Framework-CTA_IST.pdf.

requesting a 30-day extension on the comment period.[25] Once reporting is in place, it is critical that CISA and other government actors that receive this information use it to help defenders understand the actions that they can take to reduce their risks. CISA needs to be appropriately staffed and focused on this effort. In the next 18 months, entities should also employ voluntary reporting mechanisms, so that there can be a ramping up effect rather than a sudden "on switch" that dramatically changes the inflow of information to CISA.

The United States and partner governments have made strides to encourage organizations to voluntarily report ransomware incidents **(Action 4.2.3)**. Yet there remain too many potential places to report and private companies still lack clarity about which entity to alert when responding to a ransomware incident. For example, in the United States, CISA and the FBI both have portals for reporting. Europol, through its No More Ransom project portal, includes an avenue for companies to report incidents in many countries, while each EU member state is implementing reporting requirements under the NIS-2 directive in a locally adapted patchwork.[26] Governments should take on the responsibility of ensuring that if a private organization reports an incident through one portal, the information reaches all of the legally allowable recipients who would benefit from receiving the information. Private sector entities should not have to play the coordination role for the government.

Moreover, the United States and its international partners have yet to create any kind of standardized format or clearinghouse to deal with incidents **(Action 4.2.2)**. The U.S. government has acknowledged this issue and provided initial recommendations, but thus far it has not provided a concrete remedy to the problem.[27] In March 2024, DHS and the European Commission's Directorate General for Communications, Networks, Content, and Technology (DG CONNECT) announced a new initiative to compare cyber incident reporting elements and ultimately align approaches.[28] This is a welcome effort, particularly as many cyber incidents affect actors across borders. However, the initiative is in its infancy.

In the limited areas where incident reporting requirements already exist, ransomware actors are capitalizing on the opportunity to apply greater pressure to their victims to pay or risk being reported to the regulator. Shortly after the U.S. Securities and Exchange Commission (SEC) enacted new requirements for public companies to report "material" incidents within four days, a ransomware attacker filed a complaint with the Commission, alleging that one of its victims had failed to disclose the

25 The Cybersecurity Coalition et al., "Re: Request for Extension on Cyber Incident Reporting for Critical Infrastructure Act," to Mr. Todd Klessman, CIRCIA Rulemaking Team Lead, April 5, 2024, https://assets-global.website-files.com/62715f02a51b614ce64867fd/660ff63593a177d66d4c8d80_CIRCIA_ExtensionLetter_FINAL.pdf.

26 For a comprehensive overview of the development of the EU NIS-2 directive reporting requirements and some of their implications, please see: Sandra Schmitz-Berndt, Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive, *Journal of Cybersecurity*, Volume 9, Issue 1, 2023, tyad009, https://doi.org/10.1093/cybsec/tyad009.

27 U.S. Department of Homeland Security Office of Strategy, Policy, and Plans, "Harmonization of Cyber Incident Reporting to the Federal Government," September 19, 2023, https://www.dhs.gov/sites/default/files/2023-09/Harmonization%20of%20Cyber%20Incident%20Reporting%20to%20the%20Federal%20Government.pdf.

28 U.S. Department of Homeland Security, "DHS and DG CONNECT Announce Initiative Comparing Cyber Incident Reporting to Better Align Transatlantic Approaches," press release, March 20, 2024, https://www.dhs.gov/news/2024/03/20/dhs-and-dg-connect-announce-initiative-comparing-cyber-incident-reporting-better.

attack within the mandatory four day period.[29] The Commission should consider ways to disincentivize such reporting from criminal actors, such as by having a stated policy of rejecting complaints from malicious actors.[30] Without a way of countering this bad faith behavior, attackers may continue to leverage reporting requirements to extort victims, especially through the broader application of CIRCIA when it is fully implemented.

Reporting a ransom payment *before* it is made can create immense benefits to disruption efforts **(Action 4.2.4)**, as well as provide important information about the scope and scale of the crime and its broader societal impact. Governments can also take measures to respond more quickly to the ransomware incident, including issuing a freeze letter to cryptocurrency exchanges **(Action 2.1.4)**. Yet most governments also have yet to require organizations to share ransomware payment information with a government agency prior to payment. The New York Department of Financial Services has mandated ransomware payment reporting for financial services companies (23 NYCRR Part 500), but only after the fact.[31] As noted above, the SEC has also implemented reporting requirements for public companies to report "material" breaches within four days.[32] The requirement includes reporting any "material impact," which would include a ransom payment. However, the question of materiality has not been well-defined, leading many experts to worry that companies will simply delay declaring an incident "material" in order to comply with the new requirement. CIRCIA similarly requires reporting of a ransomware payment after it has been paid.

# Expanding International Collaboration

While multiple safe havens for ransomware actors exist, Russia remains the most egregious. The U.S. government is already using existing levers to deter ransomware activity in the region, including sanctions and indictments. However, since these actors serve Russia's foreign policy goals, it has few incentives to take action against them. While the ongoing conflict in Ukraine has had a mixed impact on ransomware specifically, the United States and like-minded governments are using existing policy levers to put pressure on the Russian government to reverse its full scale invasion. This means that any possible further pressure from U.S. and European governments is unlikely to be focused on combating ransomware.

The International Counter Ransomware Initiative (CRI), composed of 50+ members and with leadership from Australia, Germany, Lithuania, Nigeria, Singapore, the United Kingdom, and the United States, has committed to intensifying disruption efforts. The group includes a diverse set of governments,

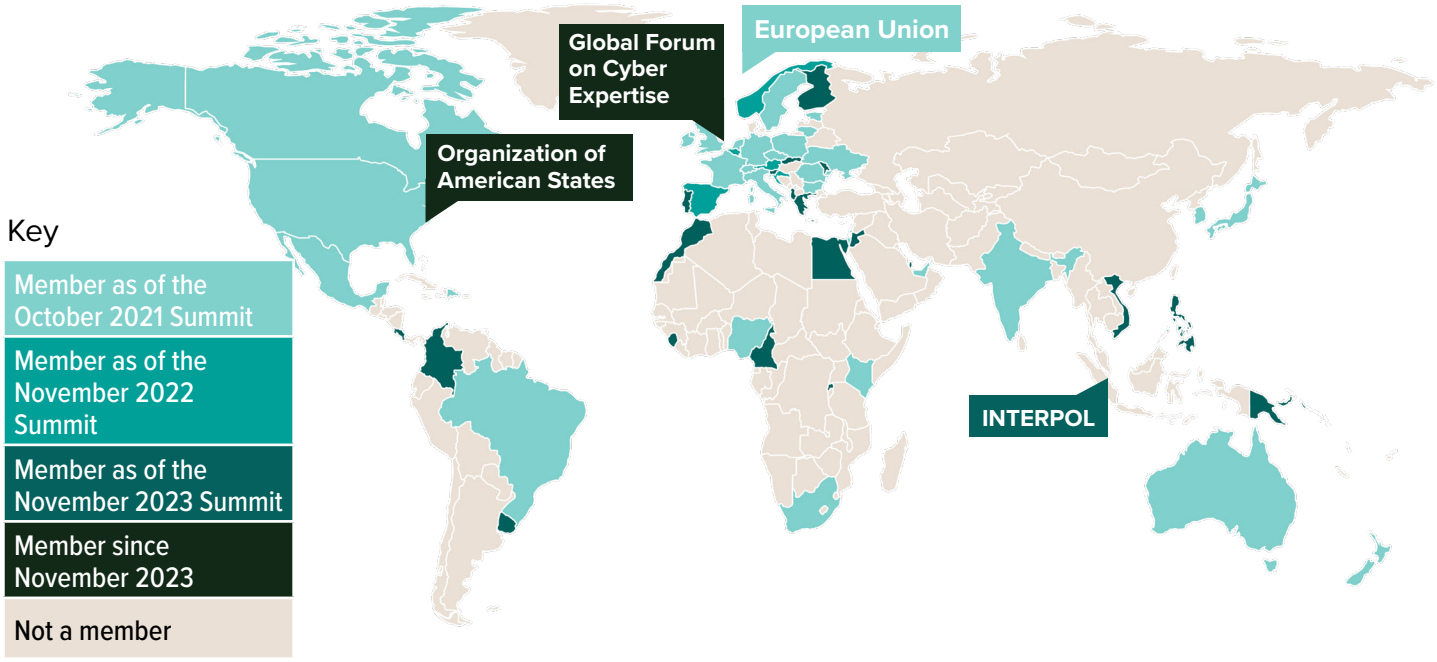
29 U.S. Securities and Exchange Commission, "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies," press release, July 26, 2023, https://www.sec.gov/news/press-release/2023-139; Jacqueline F. "Lyn" Brown, Megan L. Brown, Kathleen E. Scott, and Joshua K. Waldman, "Ransomware Attacker Files SEC Complaint to Increase Pressure on Victim," Wiley, November 17, 2023, https://www.wiley.law/alert-Ransomware-Attacker-Files-SEC-Complaint-to-Increase-Pressure-on-Victim.

30 Brown et al., "Ransomware Attacker Files SEC Complaint to Increase Pressure on Victim"; "SEC Adopts Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies."

31 New York State Department of Financial Services, Second Amendment to 23 NYCRR 500 Cybersecurity Requirements for Financial Services Companies, November 2023, 15-17, https://www.dfs.ny.gov/system/files/documents/2023/10/rf_fs_2amend23NYCRR500_text_20231101.pdf.

32 Erik Gerding, "Cybersecurity Disclosure," U.S. Securities and Exchange Commission, December 14, 2023, https://www.sec.gov/news/statement/gerding-cybersecurity-disclosure-20231214.

# CRI MEMBERSHIP GROWTH, 2021-2024[33]




with new members including Albania, Colombia, Egypt, Rwanda, and Slovakia.[34] This growing roster demonstrates increasing global commitment to combating ransomware. However, the CRI has not publicly discussed concerns around the continued existence of safe havens, and it has thus far had limited public success in shaping the behavior of governments that turn a blind eye to ransomware criminals in their midst.

To date, members of the CRI have collaborated on several prominent disruptions and takedowns.[35] For example, in August 2023, an international partnership among the United States, France, Germany, the Netherlands, the United Kingdom, Romania, and Latvia disrupted the Qakbot malware that had been used to facilitate thousands of ransomware deployments.[36] In October 2023 an international operation coordinated by Europol and Eurojust disrupted the Ragnar Locker ransomware infrastructure.[37] Eleven

33 White House, "Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting October 2021," October 14, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/14/joint-statement-of-the-ministers-and-representatives-from-the-counter-ransomware-initiative-meeting-october-2021/; White House, "International Counter Ransomware Initiative 2022 Joint Statement," November 1, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/international-counter-ransomware-initiative-2022-joint-statement/; White House, "International Counter Ransomware Initiative 2023 Joint Statement," November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/; "About the CRI," Counter Ransomware Initiative, January 27, 2024, accessed April 16, 2024, https://counter-ransomware.org/aboutus

34 "About the CRI," Counter Ransomware Initiative.

35 "LockBit cybercrime gang disrupted by CRI members," Counter Ransomware Initiative, February 22, 2024, https://counter-ransomware.org/briefingroom/b3875a4d-5484-405b-931c-c450a4fa552a.

36 United States Attorney's Office Central District of California, "Qakbot Malware Disrupted in International Cyber Takedown," press release, August 29, 2023, https://www.justice.gov/usao-cdca/pr/qakbot-malware-disrupted-international-cyber-takedown.

37 EUROPOL, "Ragnar Locker ransomware gang taken down by international police swoop," press release, October 20, 2023, https://www.europol.europa.eu/media-press/newsroom/news/ragnar-locker-ransomware-gang-taken-down-international-police-swoop.

countries, including Japan, Latvia, Spain, and the United States participated in the operation to take down the ransomware group, known for attacking critical infrastructure worldwide. And in November 2023, Europol led a coalition of seven countries to dismantle a ransomware group operating in Ukraine, leading to several arrests and detentions.[38]

CRI members are also initiating bilateral exercises focused on cyber incidents. In April 2023, the United States Treasury and the Monetary Authority of Singapore conducted an international cybersecurity exercise that aimed to help banks in both countries assess protocols for sharing information and coordinating responses to cyber incidents. These kinds of joint efforts should be expanded.[39]

However, the group has not created public formal mechanisms at regional levels to collaborate on investigative efforts. This may change over the next six months, as CRI members increase collaboration through the International Counter Ransomware Task Force (ICRTF), co-chaired by Lithuania and Australia.[40] The ICRTF will be critical for the CRI to move from a discussion venue to an information sharing mechanism. The initiative could also eventually lead to the creation of a network of ransomware investigation hubs **(Action 1.1.3)**. The White House Office of the National Cyber Director is also funding research into regional cybercrime investigation hubs as outlined by the National Cybersecurity Strategy Implementation plan.[41] Some activity under this effort may remain classified to protect sources and methods, and also to avoid alerting ransomware actors to ongoing investigative efforts. However, some information—such as the progress being made—can and should be publicized not only as a deterrent to bad actors, but also as a reminder to the public that ransomware continues to be a threat and that governments are collaborating to respond appropriately.

# Reining in Ransom Payments

One area where the CRI has made substantial progress is the public discouragement of paying ransoms, including through a commitment that national governments will not pay ransoms to extortionists.[42] The question of a possible payment ban has also resurfaced in several Western countries, including the United States, UK, and Australia. After much consideration, Australia ultimately dropped its proposed payment ban from its most recent national cybersecurity strategy, turning instead

38 EUROPOL, "International collaboration leads to dismantlement of ransomware group in Ukraine amidst ongoing war," press release, November 28, 2023, https://www.europol.europa.eu/media-press/newsroom/news/international-collaboration-leads-to-dismantlement-of-ransomware-group-in-ukraine-amidst-ongoing-war.

39 U.S. Department of the Treasury, "US Treasury and Monetary Authority of Singapore Conduct Joint Exercise to Strengthen Cross-Border Cyber Incident Coordination and Crisis Management," press release, May 1, 2023, https://home.treasury.gov/news/press-releases/jy1455.

40 "Counter Ransomware Initiative (CRI)", Australian Government Department of Home Affairs, April 8, 2024, accessed April 16, 2024, https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/counter-ransomware-taskforce.

41 "National Cybersecurity Strategy Implementation Plan," The White House, July 2023, 48 (Action 5.1.4), https://www.whitehouse.gov/wp-content/uploads/2023/07/National-Cybersecurity-Strategy-Implementation-Plan-WH.gov_.pdf.

42 Cyber Security Agency of Singapore, "International Counter Ransomware Initiative Members Come Together to Strongly Discourage Ransomware Payments," press release, November 2, 2023, https://www.csa.gov.sg/News-Events/News-Articles/2023/international-counter-ransomware-initiative-members-come-together-to-strongly-discourage-ransomware-payments.

toward designing comprehensive reporting requirements.[43] The country intends to revisit the question in two years.

In the UK, there has been public speculation and discourse on a potential payments ban,[44] though the government has provided little official comment on this beyond the December 2023 Commons Committee Report from the Joint Committee on the National Security Strategy, which states that:

> The Government's official position remains that the decision is 'ultimately a matter for the individual or organisations concerned'. Many witnesses warned against a ban, arguing it would create more shame and silence around cyber incidents. The NCA agreed, noting that 'we do not want people to pay ransoms and we will never advise people to do so', but arguing that a ban on ransoms would 'criminalize the wrong part of the equation' and would "double down" on the impact on victims. They also acknowledged that a ransom payment can sometimes be 'the only way out', and the 'lowest harm resolution to the incident'.[45]

The Ransomware Task Force Co-Chairs authored their own "Roadmap to Potential Prohibition of Ransomware Payments" (Roadmap), arguing that "a ban on payments under current circumstances will likely worsen the harms both for direct victims and, in turn, for society and the economy."[46] The roadmap notes that a payment ban would only be beneficial if governments take key actions, including efforts to better prepare the ecosystem, deter actors, improve disruption capabilities, and put in place key response and recovery mechanisms. Of the 26 original Report recommendations outlined in the Roadmap, 13 have seen limited preliminary action, while 2 have seen no known action. In other words, over half of the Roadmap recommendations are not yet fully implemented.

> "At present, the limited data available indicates that the majority of organizations globally are still underprepared to defend against or recover from a ransomware attack. This preparedness gap remains particularly problematic in resource-constrained critical sectors that are currently being heavily impacted by ransomware attacks, such as healthcare, education, and government."[47]
>
> *Roadmap to Potential Prohibition of Ransomware Payments*

43 In the Australian strategy, for example, the authors remark: "To stay ahead of the threat, we will co-design with industry options to legislate a no-fault, no-liability ransomware reporting obligation for businesses." "Australian Cyber Security Strategy: 2023-2030," Australian Government, November 22, 2023: 22, https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf; Alexander Martin, "Australia drops plans to ban ransomware payments in new national cyber strategy," *The Record*, November 22, 2023, https://therecord.media/australian-government-cybersecurity-strategy-ransomware-payments.

44 Ciaran Martin, "Cyber ransoms are too profitable. Let's make paying illegal," *The Times*, March 4, 2024, https://www.thetimes.co.uk/article/cyber-ransoms-are-too-profitable-lets-make-paying-illegal-kc8cmhxs0.

45 UK House of Commons, "A hostage to fortune: ransomware and UK national security," Joint Committee on the National Security Strategy, December 13, 2023, https://publications.parliament.uk/pa/jt5804/jtselect/jtnatsec/194/report.html#heading-3.

46 Ransomware Task Force Co-Chairs, "Roadmap to Potential Prohibition of Ransomware Payments," Institute for Security and Technology, April 10, 2024, https://securityandtechnology.org/virtual-library/memo/roadmap-to-potential-prohibition-of-ransomware-payments/.

47 "Roadmap to Potential Prohibition of Ransomware Payments."

Achieving such resilience will include incentivizing IT providers to implement secure-by-design business models that make security a core feature of their products from the very beginning. The U.S. government has pushed for an increased focus on secure-by-design in its most recent National Cybersecurity Strategy and through CISA.[48] In April 2023, Australia, Canada, New Zealand, the UK, Germany, and the Netherlands collaborated with the FBI, NSA, and CISA on a product outlining secure-by-design principles and tactics for manufacturers to follow.[49] In October 2023, CISA updated its secure-by-design guidance—in the interim period, additional countries became involved in the initiative, increasing participation to 17 international entities.[50] The OAS/CICTE CSIRTAmericas Network also became a new participant.[51]

The U.S. Department of Treasury must also work to clarify guidance surrounding ransomware payments **(Action 4.1.4)**. OFAC has updated guidance on the issue, but Task Force members still seek greater clarity to understand the implications of paying ransoms.[52] In January 2024, OFAC's senior compliance officer noted that the office wants to provide more information and is working to do so.[53] Thus far, no further action has been taken in the United States. Elsewhere, however, countries are working to provide clearer information. For example, in February 2024, the UK government published an updated guide on ransomware guidance and sanctions.[54] Many reporting venues also do not request information about cryptocurrency wallets, which limits how law enforcement can follow the money and disrupt criminals' profitability.

Governments also need to push organizations to clearly and consciously consider alternatives to payments before responding to a ransom demand **(Action 4.3.1)**. The CRI has publicly discouraged ransomware payments, and member states have committed to stopping government entities from paying ransomware extortions.[55] However, neither the CRI nor other public sector actors have developed a review process that industry and non-government entities can use to evaluate alternative mechanisms beyond payment.

Governments have taken little action to require organizations to use a standard cost-benefit analysis framework for ransomware payments **(Actions 4.3.2 and 4.3.4)**. In December 2023, the New York Department of Financial Services (NYDFS) released new requirements for financial service providers

48 "National Cybersecurity Strategy," The White House, March 2, 2023, 20, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf; "Secure by Design," CISA, accessed April 18, 2024, https://www.cisa.gov/securebydesign.

49 "Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure-by-Design and -Default," Cybersecurity and Infrastructure Security Agency, April 13, 2023, https://www.cisa.gov/sites/default/files/2023-06/principles_approaches_for_security-by-design-default_508c.pdf.

50 "Secure-by-Design—Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2024, https://www.cisa.gov/resources-tools/resources/secure-by-design.

51 "Protecting the Americas in Cyberspace," CSIRTAmerica Network, accessed April 17, 2024, https://csirtamericas.org/en.

52 U.S. Department of the Treasury, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," September 21, 2021, https://ofac.treasury.gov/media/912981/download?inline.

53 Adrianne Appel, "OFAC official urges company transparency on ransomware events," Compliance Week, January 19, 2024, https://www.complianceweek.com/sanctions/ofac-official-urges-company-transparency-on-ransomware-events/34189.article#:~:text=In%20September%202021%2C%20OFAC%20released,or%20entities%2C%20including%20ransom%20payments; Kristen Berg and Anthony Lewis, "OFAC Spotlight: Avoiding Making Ransomware Payments to Terrorists," panel, Incident Response Forum Ransomware 2024, January 18, 2024, video, https://www.youtube.com/watch?v=lbkI1muWo5o.

54 Her Majesty's Treasury Office of Financial Sanctions Implementation, "Ransomware and Sanctions: Guidance on Ransomware and Financial Sanctions," February 13, 2024, https://assets.publishing.service.gov.uk/media/65ca0d7c14b83c000ea716bd/Financial_sanctions_guidance_for_ransomware.pdf.

55 "International Counter Ransomware Initiative 2023 Joint Statement," The White House.

to report a ransomware payment within 24 hours and submit "a written description of the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control."[56] The requirements are fairly new but should facilitate information gathering for the NYDFS. Other state and federal entities should encourage this kind of cost-benefit analysis. Ideally, the NYDFS and others would require organizations to perform such activity *before* paying a ransom.

# Actions Needing Intensified Effort

In other areas, governments, industry, and civil society need to step up resource allocation and prioritize implementing existing mechanisms to the fullest extent. Key areas for further progress include active disruption, greater resilience, mechanisms to fund preparation and awareness, and more collaboration between governments and the private sector.

## Disrupting Ransomware Operations At Scale

As mentioned above, as part of their efforts to disrupt attacker groups and reduce their ability to launch attacks, the United States and other like-minded countries have conducted several substantial takedown efforts. Unfortunately, ransomware actors are resilient and in some cases are able to regroup quite quickly. Arrests and asset seizures continue to prove some of the most reliable and powerful methods for disrupting ransomware groups. When actors are operating out of safe havens and these actions are not possible, however, disruptions can still increase the costs of doing business for ransomware actors and reduce trust within the broader Ransomware-as-a-Service (RaaS) ecosystem—but to do so over the long term, these operations need to occur at scale.[57]

The U.S. government disrupted the ALPHV/Blackcat ransomware group in December 2023, only to have a variant reform and perpetrate a major attack against Change Healthcare.[58] The February 2024 takedown of the LockBit ransomware consortium also had mixed results. U.S. and UK authorities seized darknet websites run by the prolific RaaS provider, even replacing their victim-shaming website

56 New York State Department of Financial Services, "Second Amendment to 23 NY CRR 500 Cybersecurity Requirements for Financial Services Companies."

57 Andy Greenberg, "Ransomware Groups Are Bouncing Back Faster From Law Enforcement Busts," *Wired*, February 27, 2024, https://www.wired.com/story/blackcat-ransomware-disruptions-comebacks/; James Coker, "Ransomware Incidents Hit Record High, But Law Enforcement Takedowns Slow Growth," *Infosecurity Magazine*, January 30, 2024, https://www.infosecurity-magazine.com/news/ransomware-incidients-high-law/#:~:text=However%2C%20law%20enforcement%20 takedowns%20are,2022%20and%203048%20in%202021; "Q4 Ransomware Report: 2023 Ends as a Record-Breaking Year," Corvus Threat Intel, April 2, 2024, https://www.corvusinsurance.com/blog/q4-ransomware-report. The Corvus report notes, "Due to law enforcement actions, the number of ransomware leak site victims posted in Q4 2023 was, as expected, lower than Q3 (by 7%) — but still up 69% year-over-year."

58 Greenberg, "Ransomware Groups Are Bouncing Back Faster From Law Enforcement Busts."

with free incident response recovery tools. The countries were also able to seize over $110 million in unspent bitcoin being held by the group, indicting two Russian nationals and arresting several affiliates in Poland and Ukraine.[59] Additionally, authorities have been able to identify 200 affiliates from the LockBit data, in many cases matching pseudonyms with real individuals.[60] This may also generate more arrests, indictments, and sanctions. Yet the group reassembled very quickly, vowing to take even more decisive measures to target U.S. and UK critical infrastructure.[61] The United States and United Kingdom have claimed that their intensive intelligence efforts have crippled the group's long-term viability even if they do regroup, but it is too early to tell how effective such a takedown will ultimately prove.[62]

Given industry's role in the ecosystem, in order to effectively disrupt ransomware attackers, government actors also need to work closely with industry partners to increase the costs associated with the ransomware profit model. Implementing several Report recommendations could significantly improve disruption efforts, including clarifying the roles and responsibilities of industry in defending itself and sharing information with trusted government actors.

To begin, governments should clarify lawful defensive measures that the private sector can take against ransomware groups **(Action 2.2.2)**. Private companies who may be in a position to take action against malicious actor infrastructure are working to collaborate with law enforcement efforts, but they need to know what they can do without increasing their legal liability. Congress should ensure industry can take action in good faith without fear of legal liability. Specifically, Congress should work with the Executive Branch to consider whether to modernize the Computer Fraud and Abuse Act (CFAA), clarify the Cybersecurity Information Sharing Act, or amend these and other cybersecurity-related laws to account for the fact that cybersecurity providers, security researchers, and other responsible parties may need to take steps to quickly disrupt malicious attacks to protect their networks and customers.[63] Providing clearer information about how and when companies can protect themselves without fearing later legal repercussions will increase the likelihood that they do so and enhance the defense of the entire ecosystem.

As detailed in the original Report, information sharing is also a critical component for successful disruption. Governments should create more incentives for voluntary information sharing between cryptocurrency entities and law enforcement **(Action 2.1.3)**. Indeed, some of the most successful

59 Brian Krebs, "Feds Seize LockBit Ransomware Websites, Offer Decryption Tools, Troll Affiliates," Krebs on Security (blog), February 20, 2024, https://krebsonsecurity.com/2024/02/feds-seize-lockbit-ransomware-websites-offer-decryption-tools-troll-affiliates/?utm_source=pocket_saves; James Reddick, "US indicts two Russian nationals in LockBit ransomware case," *The Record*, February 20, 2024, https://therecord.media/lockbit-ransomware-indictments-us-doj-bassterlord?utm_source=pocket_saves.

60 Ryan Gallagher, "Police Scour LockBit Ransomware Evidence, Turning Up 200 Leads," *Bloomberg*, April 10, 2024, https://www.bloomberg.com/news/newsletters/2024-04-10/police-scour-lockbit-ransomware-evidence-turning-up-200-leads.

61 Scott Ikeda, "LockBit Ransomware Group Says It Is Back in Business, Debuts New Data Leak Site," *CPO Magazine*, February 28, 2024, https://www.cpomagazine.com/cyber-security/lockbit-ransomware-group-says-it-is-back-in-business-debuts-new-data-leak-site/.

62 Alexander Martin, "LockBit ransomware gang attempts to relaunch its services following takedown, *The Record*, February 26, 2024, https://therecord.media/lockbit-relaunch-attempt-follwing-takedown; Matt Burgess, "A Global Police Operation Just Took Down the Notorious LockBit Ransomware Gang," *Wired*, February 20, 2024, https://www.wired.com/story/lockbit-ransomware-takedown-website-nca-fbi/.

63 "Combating Ransomware: A Comprehensive Framework for Action," 33.

disruption efforts came about based on ad hoc cooperation rather than standardized mechanisms.[64] The Internal Revenue Service (IRS) has proposed a new rule mandating increased reporting of digital assets.[65] Should the IRS proceed, these proposed regulations would go into effect in January 2025. However, the effects of this proposed rule remain unclear. Congress is also set to reauthorize the 2015 Cybersecurity Information Sharing Act, opening up new possibilities to strengthen the resilience of the broader environment against ransomware by clarifying real and perceived gaps in the types of information covered and the types of activities authorized.

In May 2023, IST launched a Ransomware Payment Map Mini-Pilot that detailed the resourcing phase of ransomware incidents. The paper studied four threat actor case studies, outlining their path through the ransomware ecosystem and identifying the tools, services, and entities that they leveraged as they prepared for and carried out attacks. The Mini-Pilot seeks to identify which types of disruptions could be most effective in adding friction and how they could potentially be applied to the broader payment process.[66] This report helps underscore the importance of developing new levers for voluntary sharing of cryptocurrency payment indicators **(Action 2.1.1)** to ease disruption and recovery efforts.

# Fostering Public-Private Partnerships

Empowering private sector actors to mitigate ransomware threats early will improve a country's overall capacity for disruption. To be clear, the Ransomware Task Force adamantly does not support private actors taking offensive actions on other entities' networks, often referred to as "hack back." Such activity would ultimately create more harm than good. However, setting hack back aside, greater legal clarity surrounding what actions companies can take on their own networks and technical assets would be beneficial, as noted above **(Action 2.2.2)**.

Governments also need to better clarify what types of information and initiatives surrounding ransomware can be made public, and what needs to be kept private to ensure investigations and disruption efforts run smoothly. Wherever possible, governments should be actively seeking collaboration from industry and research partners, and should commit to sustained, bi-directional engagement where the government and the private sector both contribute to the collaboration. This should include efforts to exchange information, including work by the government to share relevant information with trusted members of industry and the technical community, even when such information is sensitive. Reciprocal sharing is key to building trust and establishing a cadence of ongoing collaboration. Such an approach would both signal the ongoing commitment to combat ransomware and reassure industry that their voluntary contributions are worth the investment.

64 Zoë Brammer, "Information Sharing in the Ransomware Payment Ecosystem," Institute for Security and Technology, April 17, 2024, https://securityandtechnology.org/virtual-library/reports/information-sharing-in-the-ransomware-payment-ecosystem/.

65 Internal Revenue Service, Proposed Rule, "Gross Proceeds and Basis Reporting by Brokers and Determination of Amount Realized and Basis for Digital Asset Transactions," Federal Register 88, August 29, 2023, 59576, https://www.federalregister.gov/documents/2023/08/29/2023-17565/gross-proceeds-and-basis-reporting-by-brokers-and-determination-of-amount-realized-and-basis-for.

66 Zoë Brammer, "Mapping Threat Actor Behavior in the Ransomware Payment Ecosystem: A Mini-Pilot," Institute for Security and Technology, May 2023, https://securityandtechnology.org/virtual-library/reports/mapping-threat-actor-behavior-in-the-ransomware-payment-ecosystem-a-mini-pilot/.

A key example is the Joint Ransomware Task Force (JRTF), which CIRCIA mandated. The JRTF was created to facilitate interagency cooperation **(Action 1.2.1)**.[67] CISA's website explains that the JRTF has acted to "Expand operational collaboration and multi-directional intelligence sharing between JRTF members and non-governmental partners including the private sector and the international community to more effectively prevent, detect, and respond to evolving ransomware campaigns."[68] In the first few months after its launch, the JRTF engaged openly with the researcher community to exchange information and coordinate on disruption and response efforts. However, in the months since, private sector participants have indicated that the task force's role is still somewhat ill-defined and not well understood publicly. They have shared that since the fall of 2023, government engagement via the JRTF has fallen off. If the JRTF intends only to serve as an internally facing tool, then this shift needs to be better communicated to key external stakeholders so that they can adjust their engagement with government actors accordingly.

Insurance providers are working to increase adoption of blockchain analysis technologies and services throughout the industry to drive sanctions compliance and assess possible cryptocurrency recovery and subrogation opportunities **(Action 2.1.5)**. Many insurers are also increasingly requiring that their insured entities report ransomware incidents to law enforcement (particularly the FBI's IC3) as a step in the claims process or as a condition of coverage. This activity can bolster information sharing efforts to better track and understand the broader ransomware payment ecosystem. Insurance organizations may also have an opportunity to encourage entities to report ransomware incidents *prior* to payment.

In November 2023, CISA "re-envisioned" its Cybersecurity Insurance and Data Analysis Working Group (CIDAWG) to provide an avenue for collaboration with industry, with an eye toward identifying the key security controls that are most effective at defending against cyber incidents.[69] CISA identified ransomware as a top motivator, and the threat remains a core focus area for the group. The CIDAWG aligns with an original RTF recommendation encouraging the establishment of an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management **(Action 2.1.7)**. CISA's CIDAWG is a welcome step forward; however, the group is still in its infancy and has yet to produce much in the way of tangible results.

The insurance marketplace is also an area where the United States can make significant strides toward improving prevention and response mechanisms for industry actors. CyberAcuView, an industry-supported consortium aimed at providing leadership to fight cybercrime and improve cyber resilience, aims to compile data from the insurance sector. In support of this, the consortium is developing an incident response claims taxonomy for both cyber exposure and cyber claims data to better streamline standards in incident reporting inside the insurance sector. They are also collaborating with law

67 "Joint Ransomware Task Force," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2014, https://www.cisa.gov/joint-ransomware-task-force; "Text - H.R.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022, March 15, 2022, section 106 (a), https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

68 "Joint Ransomware Task Force," Cybersecurity and Infrastructure Security Agency.

69 "Cybersecurity Insurance and Data Analysis Working Group Re-Envisioned to Help Drive Down Cyber Risk," Cybersecurity and Infrastructure Security Agency, November 20, 2023, https://www.cisa.gov/news-events/news/cybersecurity-insurance-and-data-analysis-working-group-re-envisioned-help-drive-down-cyber-risk.

enforcement agencies (FBI, INTERPOL, and others) to create information sharing opportunities within the insurance sector, including a pilot effort around disrupting and seizing ransomware payments. These steps are important moves toward improving asset recovery **(Action 2.1.5)** and information sharing across cyber insurers **(Action 2.1.7)**.

# Bolstering Resilience and Building Awareness

As noted above, some ransomware groups have begun to use more sophisticated tactics, techniques, and procedures (TTPs), including employing zero-days and targeting IT help desk infrastructure. However, the vast majority of ransomware incidents involve less sophisticated means. These incidents can be prevented through adequate preparation. Small and medium-sized enterprises continue to be about three times more likely to face a ransomware attack than larger corporations.[70] With this in mind, in 2022 the RTF Blueprint Working Group developed a *Blueprint for Ransomware Defense* ("Blueprint") that helps narrow down the most effective controls for resource-constrained organizations. The Blueprint contains a set of 40 action-oriented safeguards, drawn from the CIS Critical Security Controls Implementation Group 1 Safeguards,[71] that small- and medium-sized enterprises can implement to defend against the most common cyber attacks, including ransomware.[72] In the fall of 2023, IST published a short report testing the Blueprint's efficacy against ransomware attack points of failure, using cyber insurance claims data from provider Resilience.

> "We mapped each point of failure to a specific Blueprint Safeguard, where applicable, and determined whether or not the Safeguard, if implemented properly, could have prevented the attack. We found that at least 68% of all attacks in this particular data set could have been prevented."
>
> *Putting the Blueprint for Ransomware Defense to the Test*[73]

NIST and CISA together continue to make counter-ransomware resources available for the public. In February 2024, NIST launched its Cybersecurity Framework 2.0, which refines and strengthens NIST's guidance for how entities can evaluate their cybersecurity risks and reduce their vulnerabilities to these risks.[74] When used in collaboration with its comprehensive framework for ransomware risk

70 Eric Goldstein, "Accelerating Our Economy through Better Security: Helping America's Small Businesses Address Cyber Threats," Cybersecurity and Infrastructure Security Agency, May 2, 2023, https://www.cisa.gov/news-events/news/accelerating-our-economy-through-better-security-helping-americas-small-businesses-address-cyber.

71 "CIS Critical Security Controls Implementation Group 2," Center for Internet Security, accessed April 17, 2024, https://www.cisecurity.org/controls/implementation-groups/ig2.

72 "Blueprint for Ransomware Defense: An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises," Institute for Security and Technology, August 4, 2022, https://securityandtechnology.org/ransomwaretaskforce/blueprint-for-ransomware-defense/; "CIS Critical Security Controls Implementation Group 2."

73 Zoë Brammer, "Putting the Blueprint for Ransomware Defense to the Test," Institute for Security and Technology, August 28, 2023, https://securityandtechnology.org/blog/putting-the-blueprint-for-ransomware-defense-to-the-test/.

74 "The NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, February 26, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

management,[75] NIST offers a number of resources on its website related to ransomware preparedness measures.

Ransomware gangs continue to make use of vulnerabilities to target victim organizations. CISA's Known Exploited Vulnerabilities Catalog helps organizations prioritize patch deployment, reducing the opportunities for attackers to leverage known vulnerabilities or n-days.[76] CIRCIA also called for the establishment of a Ransomware Vulnerability Warning Pilot (RVWP), whereby CISA acts to warn critical infrastructure providers that they may have vulnerabilities that could be exploited by ransomware actors. CISA publicly launched the pilot in March 2023; by October 2023, CISA's RVWP had initiated notifications for over 800 vulnerable systems that were identified as having "internet accessible vulnerabilities commonly associated with known ransomware campaigns."[77] CISA has noted that all critical infrastructure sectors have benefited from the pilot program. CISA has continued to create new resources for the RVWP; the October 2023 refresh included a new companion list of misconfigurations and weaknesses known to be used in campaigns launched by ransomware actors.[78]

The RVWP underscores the importance of proactivity and preparation: organizations can improve their defenses against ransomware by acting quickly to mitigate known and exploitable vulnerabilities. U.S. organizations can enroll for free in CISA's vulnerability scanning program, which enables them to receive faster, targeted notifications.[79] Given available information, CISA and Congress should seek to move this effort past the pilot phase.

Following on the heels of its RVWP, CISA has also launched a Pre-Ransomware Notification Initiative to deliver critical information to potential targeted entities ahead of a ransomware attack.[80] The initiative relies critically on the Joint Ransomware Task Force (JRTF) and the Joint Cyber Defense Collaborative (JCDC), which gather actionable information from the researcher community, infrastructure providers, and cyber threat companies that is crucial to helping prevent a ransomware incident. Since ransomware actors often sit in systems for a period of time ranging from hours to days before launching an attack, these notifications can help threatened entities take crucial steps to protect themselves in advance of a ransomware attack.

The U.S. government has also made strides to improve preparedness among state and local entities

75 "Ransomware Risk Management: A Cybersecurity Framework Profile," National Institute of Standards and Technology Computer Security Resource Center, February 2022, https://csrc.nist.gov/pubs/ir/8374/final.

76 "Known Exploited Vulnerabilities Catalog," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2024, https://www.cisa.gov/known-exploited-vulnerabilities-catalog.

77 "CISA Establishes Ransomware Vulnerability Warning Pilot Program," Cybersecurity and Infrastructure Security Agency, March 13, 2023, https://www.cisa.gov/news-events/news/cisa-establishes-ransomware-vulnerability-warning-pilot-program; "Ransomware Vulnerability Warning Pilot Updates: Now A One-Stop Resource for Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware," Cybersecurity and Infrastructure Security Agency, October 12, 2023, https://www.cisa.gov/news-events/news/ransomware-vulnerability-warning-pilot-updates-now-one-stop-resource-known-exploited-vulnerabilities.

78 "Misconfigurations and Weaknesses Known to be Used in Ransomware Campaigns," Cybersecurity and Infrastructure Security Agency Stop Ransomware Portal, accessed April 17, 2024, https://www.cisa.gov/stopransomware/misconfigurations-and-weaknesses-known-be-used-ransomware-campaigns.

79 "Ransomware Vulnerability Warning Pilot Updates: Now A One-Stop Resource for Known Exploited Vulnerabilities and Misconfigurations Linked to Ransomware."

80 Clayton Romans, "Getting Ahead of the Ransomware Epidemic: CISA's Pre-Ransomware Notifications Help Organizations Stop Attacks Before Damage Occurs," Cybersecurity and Infrastructure Security Agency, March 23, 2023, https://www.cisa.gov/news-events/news/getting-ahead-ransomware-epidemic-cisas-pre-ransomware-notifications-help-organizations-stop-attacks.

**(Action 3.4.2)**. In September 2022, CISA launched the State and Local Cybersecurity Grant Program (SLCGP) and the Tribal Cybersecurity Grant Program (TCGP), which will distribute $1 billion over a four year period to states, territories, and tribes to help entities address cybersecurity risks and cyber threats to government systems.[81] Established through the Infrastructure Investment and Jobs Act of 2022, CISA and FEMA jointly manage the program. Over the past two years, these grants have been dispersed to designated state administrative authorities, seeing near full participation for eligible entities in FY22 and FY23. The Act tasks CISA with approving budget plans from grantees and dispersing money once these plans have been approved. As the first program of its kind to help recipients upgrade their networks and boost their resilience, CISA has the opportunity to assess its impact on state, local, tribal, and territorial cybersecurity. However, such an assessment will require establishing performance metrics and tracking them over time. Given the early stages of the program, no data has been made public.

## Even in a sub-optimal information environment, it's clear preparation pays so victims don't have to!

CISA's cross-sector cybersecurity performance goals[82] (CPGs) are an essential step forward in setting baseline cybersecurity best practices that apply to all sectors and particularly provide guidance for small and medium sized organizations. While not specific to ransomware, these recommendations contribute to progress in RTF **Action 3.1**, namely, "support organizations with developing practical operational capabilities." Additionally, sector-specific agencies can add value by augmenting the 38 essential CISA CPGs with relevant controls that address vulnerabilities in specific sectors.

There have also been some sector-specific efforts to provide funding for preparedness. The Department of Health and Human Services (HHS), for example, proposed investing $141 million in the Office of the Chief Information Officer for cybersecurity initiatives to align with the recent National Cybersecurity Strategy. HHS also earmarked a $1.3 billion Medicare incentive program to "encourage hospitals to adopt essential and enhanced cybersecurity practices."[83] This amount of funding is by no means sufficient, given the deep need and the broad number of healthcare services that need substantial assistance. However, it is a start to move towards assisting with preparedness.

The U.S. government has taken steps to launch an anti-ransomware campaign **(Action 1.2.3)**, but messaging remains inconsistent. In November 2023, CISA launched its "Shields Ready" campaign to increase the security and resilience of critical infrastructure.[84] The program complements its existing "Shields Up!" effort, which is a broader campaign to provide resources to organizations so they can

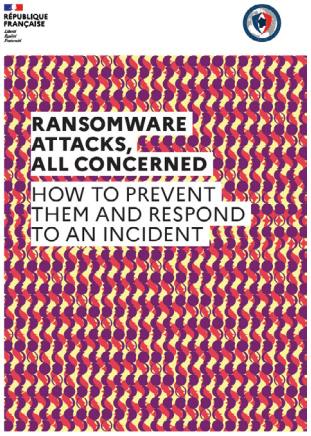
81 "State and Local Cybersecurity Grant Program," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2024, https://www.cisa.gov/state-and-local-cybersecurity-grant-program.

82 "Cross-Sector Cybersecurity Performance Goals," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2024, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

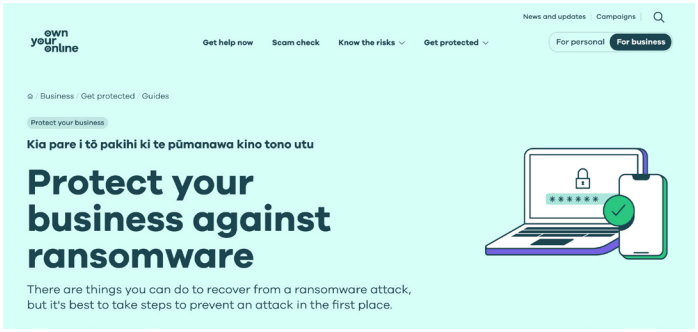
83 U.S. Department of Health and Human Services, "Fiscal Year 2025: Budget in Brief," March 2024, https://www.hhs.gov/sites/default/files/fy-2025-budget-in-brief.pdf.

84 "Factsheet: Shields Ready Campaign," Cybersecurity and Infrastructure Security Agency, November 6, 2023, https://www.cisa.gov/sites/default/files/2023-11/Factsheet-Resilience-Shields-Ready-Campaign-Nov-2023-508c.pdf.












Governments worldwide have launched campaigns spreading awareness and bolstering preparedness for ransomware attacks.

better prepare for and respond to cyber incidents, including ransomware.[85] The organization has also consolidated specific resources for ransomware incidents on its Stop Ransomware webpage **(Action 3.1.3)**.[86] Argentina, Australia, Canada, France, New Zealand, Papua New Guinea, Singapore, Switzerland, and others also provide valuable resources.[87]

However, there remains a gap in moving from offering guidance to organizations taking action. Critical infrastructure resilience varies drastically by sector (financial services companies, for example, have on average much better cybersecurity than food and agriculture or healthcare and public health sector organizations).[88] "Shields Ready" guidance is not yet sector-specific, and it does not take into account

85 "Shields Up!" Cybersecurity and Infrastructure Security Agency, accessed April 17, 2024, https://www.cisa.gov/shields-up.

86 "Stop Ransomware," Cybersecurity and Infrastructure Security Agency, April 17, 2024, https://www.cisa.gov/stopransomware.

87 "Ransomware: cómo actuar frente a un ciberataque de este tipo," [Ransomware: How to act against a cyber attack of this type], Government of Argentina, accessed April 17, 2024, https://www.argentina.gob.ar/jefatura/innovacion-publica/ssetic/direccion-nacional-ciberseguridad/cert-ar/publicaciones-0; "Ransomware," Australian Government, accessed April 17, 2024, https://www.cyber.gov.au/threats/types-threats/ransomware; "Ransomware playbook (ITSM.00.099)," Government of Canada, accessed April 17, 2024, https://www.cyber.gc.ca/en/guidance/ransomware-playbook-itsm00099; "Ransomware attacks, all concerned - How to prevent them and respond to an incident," French Republic, accessed April 17, 2024, https://cyber.gouv.fr/node/4740; "Protecting from ransomware," Computer Emergency Response Team New Zealand, accessed April 17, 2024, https://www.cert.govt.nz/business/guides/protecting-from-ransomware/; "Ransomware," Papua New Guinea Computer Emergency Response Team, accessed April 17, 2024, https://www.pngcert.org.pg/common-threats/ransomware/; "SPF | Ransomware," Cyber Security Agency of Singapore, accessed April 17, 2024, https://www.police.gov.sg/Advisories/Crime/Cybercrime/Ransomware; "Ransomware," National Cyber Security Centre, accessed April 17, 2024, https://www.ncsc.admin.ch/ncsc/en/home/cyberbedrohungen/ransomware.html.

88 President's Council of Advisors on Science and Technology, "Report to the President: Strategy for Cyber-Physical Resilience–Fortifying Our Critical Infrastructure for a Digital World," Executive Office of the President, February 2024, https://www.whitehouse.gov/wp-content/uploads/2024/02/PCAST_Cyber-Physical-Resilience-Report_Feb2024.pdf.

the very different ecosystems and challenges faced by under-resourced critical infrastructure. The CRI has also created a website with comprehensive international advisories, but it does not provide additional ransomware prevention resources.[89]

The same is true of CISA's efforts to provide tabletop exercises for critical infrastructure sectors **(Action 3.2.2)**. CISA provided a ransomware tabletop exercise in September 2023, but the guidance is not broken out by sector. Currently, the materials provide brief case studies for government facilities services, chip manufacturing, telecommunications, and healthcare.[90] Right now, however, the information is limited and does not provide actionable advice for the sectors mentioned. Additionally, CISA has yet to lead efforts with sector risk management agencies to put these exercises into practice. In Spring 2024, CISA will be conducting its biennial Cyber Storm exercise, which will explicitly focus on critical infrastructure sectors and their cybersecurity interlinkages.[91]

Governments can also do more to draw attention to the worst actors. The CRI is working to create a shared denylist of cryptocurrency wallets known to belong to ransomware actors.[92] The original Report recommended creating target decks of ransomware developers, criminal affiliates, and ransomware variants to help improve public awareness around key threats in this space **(Action 2.3.2)**. These decks can consist of consolidated lists of central members of the most dangerous ransomware groups, ranked by their centrality: leaders of ALPHV/Blackcat, for example, could be the suit of hearts, with leaders as face cards and prominent but lesser members as lower ranked cards. The suit-style target deck helps underscore to governments and the private sector that these gangs are high priorities for disruption, that organizations should avoid paying ransoms to them, and that these groups are clear targets for indictments and arrests over the long haul.

With other crimes, the United States has publicized top threat actors through the FBI's most wanted list and other similar approaches. A public counter ransomware program could help make combating this activity a priority for households. The FBI does currently have a "Cyber's Most Wanted" webpage, although it does not denote ransomware actors in particular.[93] In the international context, the U.S. State Department has used its Rewards for Justice program to bring attention to some of the most prominent ransomware groups.[94] Globally, Europol's EC3's efforts to collaborate with the private sector include work to develop priorities for investigation and prosecution, but those are not publicly disclosed.[95]

89 "International Counter Ransomware Initiative," Counter Ransomware Initiative, accessed April 17, 2024, https://counter-ransomware.org/.

90 "CISA Tabletop Exercise Package Ransomware," Cybersecurity and Infrastructure Security Agency, September 2023, 21-23, https://docs.google.com/viewer?url=https%3A%2F%2Fwww.cisa.gov%2Fsites%2Fdefault%2Ffiles%2F2023-09%2FRansomware-CTEP-Situation-Manual-092023-508.docx.

91 "Cyber Storm IX: National Cyber Exercise," Cybersecurity and Infrastructure Security Agency, accessed April 17, 2024, https://www.cisa.gov/cyber-storm-ix-national-cyber-exercise.

92 "International Counter Ransomware Initiative 2023 Joint Statement," The White House, November 1, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

93 "Cyber's Most Wanted," Federal Bureau of Investigation, accessed April 17, 2024, https://www.fbi.gov/wanted/cyber.

94 "Index - Rewards for Justice," U.S. Department of State, accessed April 17, 2024, https://rewardsforjustice.net/index/?jsf=jet-engine:rewards-grid&tax=cyber:857%2C3266.

95 Elizabeth Vish and Georgeanela Flores Bustamante, "Public Private Partnerships to Combat Ransomware: An inquiry into three case studies and best practices," Institute for Security and Technology, March 28, 2024, https://securityandtechnology.org/wp-content/uploads/2024/04/Public-Private-Partnerships-to-Combat-Ransomware-GFCEIST.pdf.

The public does not have access to detailed information about whether these notices have led to actionable intelligence. If threat hunters and others in the public knew more about how these programs effectively work, the government could get higher quantities and qualities of tips that could be leveraged to exert more significant impact across the ransomware ecosystem. Additionally, Rewards for Justice—as well as inclusion on sanctions lists—generally take substantial time to develop. A faster moving process, which could later be tied to other programs, would help victims and threat hunters move at a pace closer to that of criminals swapping aliases.

# Committing Financial Resources to Preparation and Response

As the U.S. government considers what additional tools to leverage to combat ransomware, it should further explore alleviating fines for critical infrastructure entities that align with the Ransomware Framework **(Action 3.4.4)**, which should be tailored to each sector. In September 2021, the Treasury Department's Office of Foreign Assets Control (OFAC) attempted to make progress in this area through its advisories.[96] However, no other U.S. government entity has yet followed suit.

The U.S. government should also investigate tax break systems for organizations that comply with current cybersecurity guidance. In 2013, the U.S. Department of Commerce issued a set of recommendations around cybersecurity incentive structures, ultimately deeming tax breaks to be insufficient and thus not worth pursuing at the time.[97] The climate has shifted significantly in the last ten years. The 2023 National Cybersecurity Strategy stated explicitly that other sectors are encouraged to implement strong incentive programs for cybersecurity compliance, including tax structure changes. The strategy further notes that "In seeking new regulatory authority, the Administration will work with Congress to develop regulatory frameworks that take into account the resources necessary to implement them."[98] The National Cybersecurity Implementation Plan also made reference to working with international partners to push for the adoption of regulatory frameworks for secure ICT systems, using International Security Technology and Innovation Funding.[99]

Thus far, however, no major tax incentive structures have been implemented at the federal (or global) level. In 2018, Maryland established the Buy Maryland Cybersecurity (BMC) Tax Credit for qualified companies purchasing and selling cybersecurity technologies and services. A qualified company purchasing cybersecurity technologies or services from a qualified seller can claim a tax credit of up to 50% of the cost of purchasing such services, up to $50,000 per qualified buyer. Qualified cybersecurity sellers can aggregate up to $200,000 in tax credits before they are deemed ineligible for further

96 U.S. Department of the Treasury, "Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," September 21, 2021, https://ofac.treasury.gov/media/912981/download?inline.

97 U.S. Department of Commerce, "Discussion of Recommendations to the President on Incentives for Critical Infrastructure Owners and Operations to Join a Voluntary Cybersecurity Program," August 6, 2013, https://www.ntia.doc.gov/files/ntia/Commerce_Incentives_Discussion_Final.pdf.

98 "National Cybersecurity Strategy," The White House, 9.

99 "National Cybersecurity Strategy Implementation Plan," The White House.

credits in that tax year.[100] As of June 2023, 86 businesses have been awarded a total of $2.1 million in credits. While an evaluation conducted by the Maryland Office of Policy Analysis recommended the termination of the tax credit due to underutilization, the evaluation further recommends raising awareness of the program should the Maryland General Assembly choose to continue offering this tax credit.[101] The Maryland experiment, while not yet a full success story, offers a useful potential model for further exploration. Given the distributed nature of the cybersecurity ecosystem, a federal tax break may be required for such a system to work at full capacity.

Federal agencies should continue to pursue opportunities to require local governments to adopt limited baseline security measures **(Action 3.3.2)**. Some initial efforts have attempted to enforce baseline security measures within a few sector-specific agencies. For example, HHS has outlined a limited sub-set of CISA's CPGs that they are seeking to require healthcare providers to adopt as cybersecurity goals. These include some, but not all, of the truly essential cybersecurity best practices outlined in CISA's CPGs. Because HHS has regulatory authority, and because health care is often targeted and life-critical, it is crucially important that HHS requirements be comprehensive enough to provide a reasonable assurance that regulated entities implement minimum best practices. The U.S. government should also explore requiring managed service providers to adopt similar baseline measures **(Action 3.3.3)**. In May 2022, CISA announced a joint cyber advisory that urged MSPs and their customers to implement baseline cybersecurity measures and operational controls.[102] However, nothing has yet been mandated for MSPs.

Existing response mechanisms are particularly under-publicized and underutilized. The November 2021 Cyber Response and Recovery Act (CRRA) established several important measures, including authorizing the Secretary of DHS, in consultation with the National Cyber Director, to declare a significant cyber incident **(Action 4.1.1)**.[103] Such a declaration can be made when a particular incident has happened or is deemed to be imminent and when there are insufficient funds available to provide adequate preparation. Yet based on publicly available information, these authorities have yet to be used or tested in any meaningful way, even during events that may have fulfilled the relevant criteria—an incident that "results, or is likely to result, in demonstrable harm" to national security interests or public confidence and safety.[104] The CRRA also created a Cyber Response and Recovery Fund **(Action 4.1.2)** with $100 million available through September 2028 to support response efforts in the event of a significant cyber incident.[105] Since there has been no significant cyber incident declared, these funds have likely not been put to use.

---

100 Maryland Department of Legislative Services, "Evaluation of the Credit for the Purchase of Cybersecurity Technology or Services," December 2023, https://dls.maryland.gov/pubs/prod/TaxFiscalPlan/Evaluation_Credit_for_Purchase_of_Cybersecurity_Technology_or_Services.pdf.

101 Maryland Department of Legislative Services, "Evaluation of the Credit for the Purchase of Cybersecurity Technology or Services."

102 "Protecting Against Cyber Threats to Managed Service Providers and Their Customers," Cybersecurity and Infrastructure Security Agency, May 11, 2022, https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-131a.

103 "Text - H.R.3684 - 117th Congress (2021-2022): Infrastructure Investment and Jobs Act," November 15, 2021, section 2233 (a), https://www.congress.gov/bill/117th-congress/house-bill/3684/text.

104 "Text - H.R.3684 - 117th Congress (2021-2022): Infrastructure Investment and Jobs Act," section 2232.

105 "Text - H.R.3684 - 117th Congress (2021-2022): Infrastructure Investment and Jobs Act," section 2234(a).

Other than the Cyber Recovery and Response Fund described above, publicly available information does not suggest the United States has made significant progress in increasing government resources available to help the private sector respond to ransomware attacks **(Action 4.1.3)**. The RTF called for additional government staff to be allocated to respond specifically to ransomware. Thus far, the U.S. government has made few apparent moves to do so. In June 2023, the U.S. Department of Justice merged its cryptocurrency and computer crimes investigative units.[106] The Justice Department also established the National Security Cyber Section in the National Security Division, another positive move toward prioritizing ransomware incidents.[107] These actions are a good step forward, but they do not necessarily free up additional employees to work on the issue and do not represent the kind of extensive resource allocation needed.

The U.S. government needs to provide assistance to ransomware victims—particularly those in under-resourced critical infrastructure sectors. As the RTF co-chairs noted in the Roadmap, "Additionally, governments and the technical community need to strengthen victim support to give organizations who are affected by attacks alternative options for recovery beyond paying the ransom."[108] Particularly for critical infrastructure that is under-resourced, the government should seek to meet victims where they are to look at options to reconstitute critical systems without relying on the criminals to decrypt systems.

# Conclusion

As this Progress Report makes clear, governments, civil society, the technical community, and the private sector have made strides in tackling ransomware and have outlined plans to continue to do so. Yet reports of ransomware—including massive payments to criminals—continue to rise. This rise does not necessarily imply increasing criminal activity; rather, it could signal that efforts to encourage greater transparency and reporting are paying off, or that attackers are increasingly focused on more public-facing activity, such as selling information. Until we have a solid baseline of data, it will be nearly impossible to draw accurate conclusions. However, we can confidently conclude that, given the continued increase in reported incidents, for the time being, we have not solved this problem. Achieving progress on the remaining 24 RTF recommendations will help address the ransomware threat, and the U.S. and other governments worldwide will need to continue to act going forward. At the same time, they should work toward driving adoption of secure-by-design and -default across the ecosystem.

Based on the original RTF Report recommendations, the U.S. government and like-minded partners need to continue to commit additional resources to disruption efforts, strengthening focus and

106 Paul Elias, "DOJ merges cyber, cryptocurrency units to go after ransomware attacks," SC Magazine, July 21, 2023, https://www.scmagazine.com/news/doj-merges-cyber-cryptocurrency-units-to-go-after-ransomware-attacks.

107 "Justice Department Announces New National Security Cyber Section Within the National Security Division," U.S. Department of Justice, June 20, 2023, https://www.justice.gov/opa/pr/justice-department-announces-new-national-security-cyber-section-within-national-security.

108 RTF Co-Chairs, "Roadmap to Potential Prohibition of Ransomware Payments."

collaboration across borders **(Action 1.1.3, Action 2.1.3, Action 2.1.5, Action 2.2.1)**. Public-private partnerships need renewed investments **(Action 2.1.1, Action 2.1.3, Action 2.1.7)**. Governments also need to make more concerted efforts to create streamlined awareness and resilience for organizations, particularly under-resourced SMEs **(Action 1.2.3, Action 2.2.2, Action 2.3.2, Action 3.1.3, Action 3.2.2, Action 3.3.2)**. The U.S. government also needs to improve financial incentives for preparation and resources for victim organizations **(Action 3.4.4, Action 3.4.5, Action 4.1.3)**. Finally, the United States and other governments need to commit and invest in existing mechanisms, including CIRCIA, the JRTF, the JCDC, and the CRI to drive more impact **(Action 2.1.1, Action 2.1.3, Action 4.2.2, Action 4.2.3, Action 4.2.4, Actions 4.3)**.

The RTF will continue to focus on bringing together key international stakeholders across industry, government, and civil society to address these challenges. We will push for actionable steps to reduce the risks of ransomware and help safeguard our societies from this growing threat.

# GOAL 1: DETER RANSOMWARE ATTACKS

| Objective | Rec. | Description | Lead | Timeline |
|---|---|---|---|---|
| Signal that ransomware is an international diplomatic and enforcement priority | 1.1.1 | **Issue declarative policy through coordinated international diplomatic statements that ransomware is an enforcement priority.** | National governments | Begin groundwork immediately; declarations to be issued upon international group meeting |
| | 1.1.2 | **Establish an international coalition to combat ransomware criminals.** | U.S. lead, in coordination with international partners | 3-6 months |
| | 1.1.3 | **Create a global network of ransomware investigation hubs.** | U.S. lead, in coordination with international partners | 9-12 months |
| | 1.1.4 | **Convey the international priority of collective action on ransomware via sustained communications by national leaders.** | White House | Begin groundwork immediately; declarations ongoing |
| Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House | 1.2.1 | **Establish an Interagency Working Group for ransomware.** | White House / NSC | Immediate |
| | 1.2.2 | **Establish an operationally focused U.S. government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub.** | White House in coordiation with private industry | Immediate |
| | 1.2.3 | **Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign.** | White House in coordiation with private industry | 3-6 months |
| | 1.2.4 | **Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public.** | DOJ and congress, in coordination with international equivalents | 9-12 months |
| | 1.2.5 | **Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat.** | White House (via DNI) | 3 months |
| | 1.2.6 | **Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns.** | White House (via DNI), coordinate with Five Eyes partners | 3 months |
| Substantially reduce safe havens where ransomware actors currently operate with impunity | 1.3.1 | **Exert pressure on nations that are complicit or refuse to take action.** | DOJ and DOS | 3 months, ongoing |
| | 1.3.2 | **Incentivize cooperation and proactive action in resource-constrained countries.** | DOJ and DOS, coordinate with international equivalents | 30 days, ongoing |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION

# GOAL 2: DISRUPT THE RANSOMWARE BUSINESS MODEL

| Objective | Rec. | Description | Lead | Timeline |
|---|---|---|---|---|
| Disrupt the system that facilitates the payment of ransoms | 2.1.1 | **Develop new levers for voluntary sharing of cryptocurrency payment indicators.** | Congress, CISA, international equivalents | 6-12 months |
| | 2.1.2 | **Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws.** | U.S. Treasury, SEC, international equivalents | 12 months |
| | 2.1.3 | **Incentivize voluntary information sharing between cryptocurrency entities and law enforcement** | U.S. Treasury (FinCEN) | 12 months |
| | 2.1.4 | **Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes.** | U.S. DOJ and international equivalents | 6-12 months |
| | 2.1.5 | **Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation.** | U.S. and international insurance and re-insurance firms | 6-12 months |
| | 2.1.6 | **Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs.** | SEC and international equivalents | 6-12 months |
| | 2.1.7 | **Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.** | U.S. and international insurance and re-insurance firms | 6-12 months (to establish consortium and initial subrogation effort) |
| Target the infrastructure used by ransomware criminals | 2.2.1 | **Leverage the global network of ransomware investigation hubs.** | USG and international equivalents | 6-12 months |
| | 2.2.2 | **Clarify lawful defensive measures that private-sector actors can take when countering ransomware.** | Congress | 12-24 months |
| Substantially reduce safe havens where ransomware actors currently operate with impunity | 2.3.1 | **Increase government sharing of ransomware intelligence.** | DHS | 6 months, ongoing |
| | 2.3.2 | **Create target decks of ransomware developers, criminal affiliates, and ransomware variants.** | USG and national governments | 6-12 months |
| | 2.3.3 | **Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure.** | U.S. law enforcement and international equivalents | 12-24 months |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION

# GOAL 3: HELP ORGANIZATIONS PREPARE

| Objective | Rec. | Description | Lead | Timeline |
|---|---|---|---|---|
| Support organizations with developing practical operational capabilities | 3.1.1 | **Develop a clear, actionable framework for ransomware mitigation, response, and recovery.** | NIST, int'l equivalents, private sector participation | 12-24 months, updated yearly thereafter |
| | 3.1.2 | **Develop complementary materials to support widespread adoption of the Ransomware Framework.** | NIST and international equivalents | 12-24 months, updated regularly thereafter |
| | 3.1.3 | **Highlight available internet resources to decrease confusion and complexity.** | Internet search companies, along with nonprofit input | 6-12 months for first iteration, ongoing thereafter |
| Increase knowledge and prioritization among organizational leaders | 3.2.1 | **Develop business-level materials oriented toward organizational leaders.** | CISA | 6-12 months, with updates yearly as needed |
| | 3.2.2 | **Run nationwide, government- backed awareness campaigns and tabletop exercises.** | USG and int'l equivalents, appropriate agency leads, organizational partners | 12-24 months, ongoing for as long as relevant |
| Update existing, or introduce new, cybersecurity regulations to address ransomware | 3.3.1 | **Update cyber-hygiene regulations and standards.** | State/Federal governments; support from state/local entities | Likely 12-24 months, with subsequent iterations |
| | 3.3.2 | **Require local governments to adopt limited baseline security measures.** | USG and international equivalents | 6-12 months, updated yearly thereafter |
| | 3.3.3 | **Require managed service providers to adopt and provide baseline security measures.** | Congress and international legislatures | 6-12 months |
| Financially incentivize adoption of ransomware mitigations | 3.4.1 | **Highlight ransomware as a priority in existing funding provisions.** | Relevant fund designation agencies | 3-6 months |
| | 3.4.2 | **Expand Homeland Security Preparedness Grants to encompass cybersecurity threats.** | DHS working with Congress | 6-12 months |
| | 3.4.3 | **Offer local government, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework.** | USG and international equivalents | Likely 12-24 months |
| | 3.4.4 | **Alleviate fines for critical infrastructure entities that align with the Ransomware Framework.** | USG and international equivalents | 12-24 months |
| | 3.4.5 | **Investigate tax breaks as an incentive for organizations to adopt secure IT services.** | USG and international equivalents | 24 months |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION

# GOAL 4: RESPOND TO RANSOMWARE ATTACKS

| Objective | Rec. | Description | Lead | Timeline |
|---|---|---|---|---|
| Increase support for ransomware victims | 4.1.1 | **Create ransomware emergency response authorities.** | USG and international equivalents | 12-24 months |
| | 4.1.2 | **Create a Ransomware Response Fund to support victims in refusing to make ransomware payments.** | USG, insurance industry | 12-24 months |
| | 4.1.3 | **Increase government resources available to help the private sector respond to ransomware attacks.** | USG and international equivalents | 12-24 months |
| | 4.1.4 | **Clarify United States Treasury guidance regarding ransomware payments.** | US Treasury | 6-12 months |
| Increase the quality and volume of information about ransomware incidents | 4.2.1 | **Establish a Ransomware Incident Response Network (RIRN).** | A nonprofit and international equivalents | 12-24 months to reach full operational capacity |
| | 4.2.2 | **Create a standard format for ransomware incident reporting.** | A nonprofit and international equivalents | 6-12 months |
| | 4.2.3 | **Encourage organizations to report ransomware incidents.** | DHS/CISA | 6-12 months, ongoing as needed |
| | 4.2.4 | **Require organizations and incident response entities to share ransomware payment information with a national government prior to payment.** | USG and international equivalents | 12-24 months |
| Require organizations to consider alternatives to paying ransoms | 4.3.1 | **Require organizations to review alternatives before making payments.** | USG and international equivalents | 12-24 months |
| | 4.3.2 | **Require organizations to conduct a cost-benefit assessment prior to making a ransom payment.** | USG and international equivalents | 12-24 months |
| | 4.3.3 | **Develop a standard cost-benefit analysis matrix.** | NIST and international equivalents, private sector participation | 12-24 months |

SIGNIFICANT ACTION UNDERWAY  PRELIMINARY ACTION NOTED  NO KNOWN ACTION

RANSOMWARE
TASK FORCE

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org