THE RANSOMWARE TASK FORCE
GAINING GROUND

MAY 2023 PROGRESS REPORT

RANSOMWARE
TASK FORCE

THE RANSOMWARE TASK FORCE: GAINING GROUND

RANSOMWARE
TASK FORCE

May 2023

Table of Contents

Introduction

In April 2021, the Ransomware Task Force (RTF) published *Combating Ransomware: A Comprehensive Framework for Action* ("2021 RTF report") with 48 recommendations for government, industry, and civil society designed around four pillars to **deter** and **disrupt** the ransomware model and help organizations **prepare** for and **respond** to attacks at scale. Two years later, we have seen impressive moves by industry, U.S., and partner governments toward implementing these recommendations. In particular, we have seen continued commitment to combat this threat through the following actions:

- Increasing public-private and government-to-government collaboration on disruptive activity
- Increasing focus on reporting and information sharing
- Ongoing efforts to reduce some of the risks posed by cryptocurrency

We have also seen significant change across the ransomware landscape. Governments have taken action to prioritize ransomware defenses and investigations; victims have changed their responses; and threat actors have evolved, not only in terms of who they affiliate with, but also in terms of their tactics and the size and geographic location of their targets.

For example, according to research from CrowdStrike, the use of ransomware itself was down 20% in data theft and extortion campaigns during 2022, indicating that encryption was becoming less appealing to threat actors as threats of data leaks rise. In another sign of effective action against the ransomware threat, Chainalysis reported that the average lifespan of a ransomware strain in 2022 was 70 days, down from 153 days in 2021 and 265 in 2020.

Beyond this, in the first half of 2022, there appeared to be a significant decrease in attacks against the organizations in the United States and other countries that have typically topped the charts for reported incidents. This seems to be in part a side effect of the Russian invasion of Ukraine, which has disrupted and redirected the focus of many cybercriminal groups based in the region.

Despite this, ransomware remains a major threat to both companies and civil society, with reports of increasing numbers of attacks against organizations in Latin America and Asia.[1] According to an Emsisoft report, ransomware impacted 2,025 educational institutions, 290 hospitals, and 105 local governments in the United States in 2022. Ransomware also continues

[1] According to IBM's 2022 Threat Intelligence report, Asia became the most attacked region globally in 2022, surpassing both North America and Europe. Latin America's share of attacks identified in that report increased significantly, from 9 to 13 percent of global attacks, and Latin American countries were the first and second most attacked. See IBM, "X-Force Threat Intelligence Index 2022," May 2022, https://www.ibm.com/downloads/cas/ADLMYLAZ.

to take an economic toll: the average ransomware payment in Q4 2022 was $408,644 USD, up 58% from Q3 2022 according to Coveware. According to an April 2023 Sophos report, over two-thirds (68%) of incidents recorded in this year's Active Adversary data were ransomware attacks.

This report walks readers through the RTF's second year, acknowledging tremendous shifts in the ecosystem, especially in light of the war in Ukraine, and highlights key areas of progress. Whereas last year's progress report captured the early wins of an anti-ransomware campaign, this year we grappled with the more elusive goal of sustaining success against evolving challenges.

Lastly, this report also outlines areas to watch in the next year, including:

» Sustaining focus on collecting and sharing ransomware data

» Improving baseline cybersecurity across the ecosystem

» Reexamining existing incentive structures

Progress Overview

When IST established the RTF in December 2020, we knew that there would be no easy solution to counter the ransomware threat. Against the backdrop of escalating consequences and the increasing prevalence of ransomware attacks on critical and significant systems, we saw an urgent need to bring together experts in industry, policy, law enforcement, and cyber insurance, along with members of civil society and international organizations to design recommendations to address the threat.

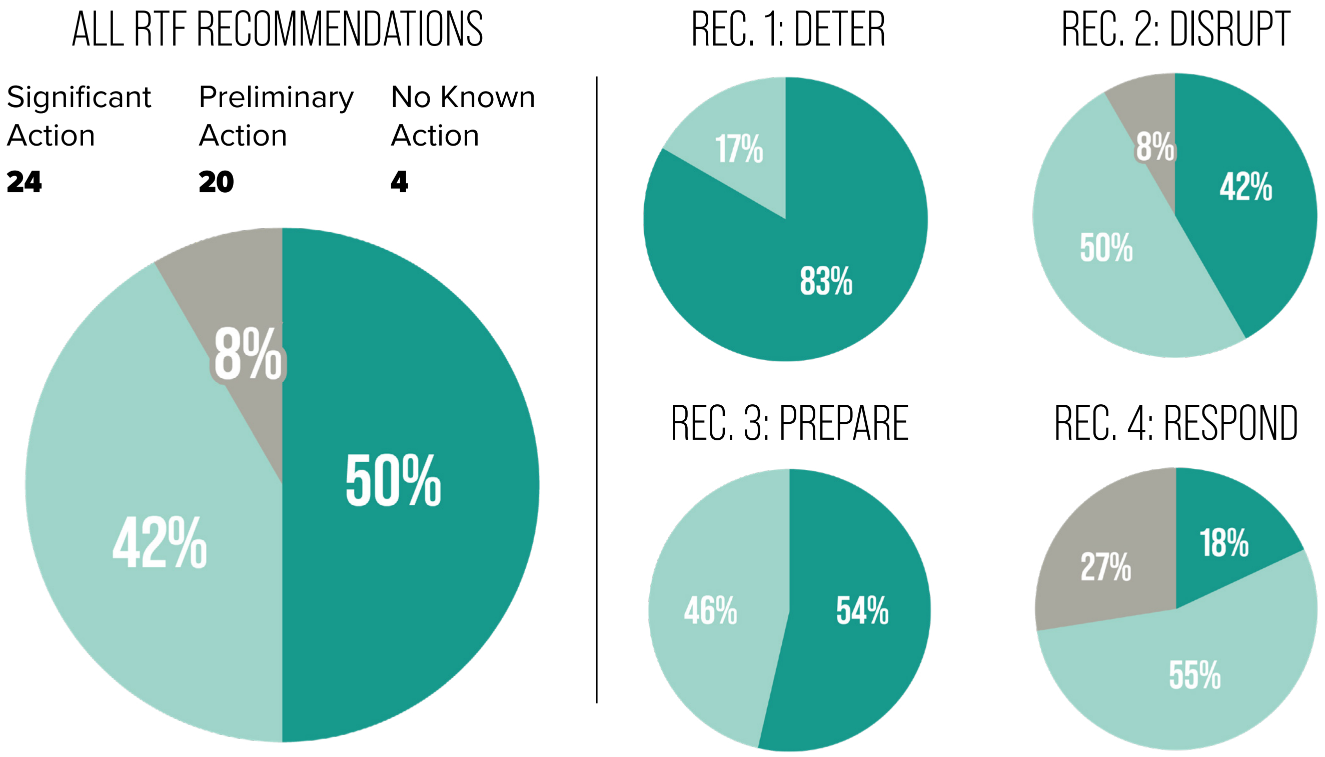
Despite numerous challenges and conflicting priorities, we have seen increasing government engagement on this issue in many countries around the world. Many have adopted or are exploring measures discussed in the original RTF report, as outlined in this paper.

As of May 2023, 92% of the 48 RTF recommendations have seen some action, with 50% experiencing significant progress, including through legislation and policy adoption.

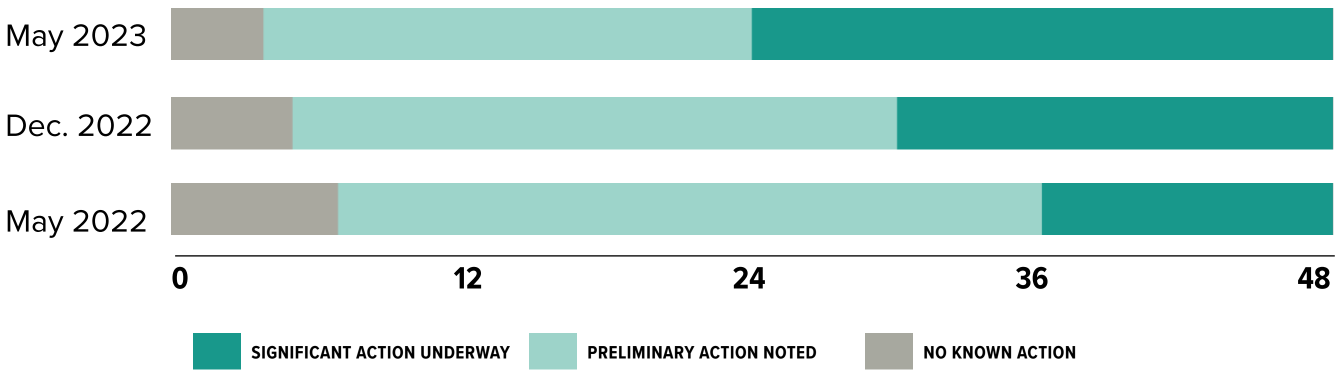
Of the 48 specific recommendations, 24 have seen significant progress in the two years since the 2021 RTF report's release. Preliminary actions have been observed on 20 more, while only 4 recommendations have had no publicly known action.

This year, we began evaluating recommendations with less precisely measurable outcomes. For example, “conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign” **(Action 1.2.3)** facilitates ongoing processes that are not easily confined to the “complete” / “incomplete” binary. Additionally, we know that progress on some recommendations happens behind the scenes – we may never know, for example, if governments are leveraging a “global network of ransomware investigation hubs” **(Action 1.1.3)**.

RTF RECOMMENDATIONS: MAY 2023 STATUS



OVERALL PROGRESS: MAY 2022 - MAY 2023



An Evolving Landscape: Ransomware Numbers and the War in Ukraine

The cybercrime ecosystem continues to evolve rapidly. One of the defining factors of the 2022-23 ransomware landscape is the ongoing war in Ukraine, which is especially impactful given the high concentration of cybercrime groups emanating from Russia and its neighbors. In the immediate months following the invasion, we witnessed a shift in the scale and focus of ransomware and other cybercrime, signaling a change in the priorities of and constraints on actors in the space.

While the conflict has not delivered the full-fledged cyber war that some commentators predicted, cyber attacks against Ukraine have been constant and substantial both leading up to and during the invasion, and have also been an active part of Ukraine's own defensive operations.

One possible side effect of the war is a refocusing of the efforts of cybercriminals from Russia and its near abroad in two directions. First, there is a public presumption that the efforts of some criminal actors have been redirected from lucrative cybercrime like ransomware attacks toward contributions to wartime operations.

Additionally, while ransomware activities emanating from Russia and its near abroad have continued, these cybercrime groups also appear to be expanding their targets to include a greater emphasis on the Global South, including by shifting toward Asian and Latin American targets and away from critical infrastructure and other sensitive targets within NATO countries.[2] This refocusing away from critical infrastructure and other sensitive targets in NATO countries may be driven by a desire to avoid incidents that could increase friction between Russia and NATO countries.

The long term implications of the invasion for the cybersecurity ecosystem are uncertain. A few outstanding questions include how this conflict impacts safe harbors for cybercriminals and what the cybercrime ecosystem will look like as the conflict between Ukraine and Russia evolves. Moreover, as the conflict wears on, additional reporting blurs our understanding of the overall direction of ransomware. As we said last year, the picture remains incomplete.

[2] See, for example, recent attacks in Costa Rica and Japan: "Cybercrime in Japan hits record high in 2022 as ransomware cases surge," *The Japan Times*, September 15, 2022, https://www.japantimes.co.jp/news/2022/09/15/national/crime-legal/ransomeware-attacks-rise/; Insikt Group, "Latin American Governments Targeted By Ransomware," *Recorded Future*, June 14, 2022, https://www.recordedfuture.com/latin-american-governments-targeted-by-ransomware.

Increasing Public-Private and Government-to-Government Collaboration

This year, we welcomed increased public-private and government-to-government collaboration on disruptive activity. In the 2021 RTF report, we called for ransomware to be recognized as a threat to national security and to "convey the international priority of collective action on ransomware via sustained communications by national leaders" **(Action 1.1.4)**. The U.S. government continues to prioritize ransomware as a critical threat **(Actions 1.1.1; 1.1.4)**; for example, the 2023 U.S. National Cybersecurity Strategy includes the defeat of ransomware as a strategic objective and "recognizes that robust collaboration, particularly between the public and private sectors, is essential to securing cyberspace" **(Action 1.2.3)**. U.S. and partner governments continue to push forward a cross-sector response to ransomware including education and awareness campaigns like the State Department's Quad Cyber Challenge; the dissemination of threat intelligence including CISA's ransomware-related joint cybersecurity advisories; disruptive campaigns by law enforcement; sanctions against cybercrime gangs like Trickbot, illicit marketplaces like Genesis, and cryptocurrency mixers like Blender.io; as well as reporting requirements.

We have seen a number of joint investigative efforts over the past year. In January, 2023, Europol and partners in France, Spain, Portugal, and Cyprus, together with U.S. authorities dismantled Bitzlato, a cryptocurrency exchange that had received over $15 million in ransomware payments. In March 2023, the U.S. Department of Justice (DOJ) announced the takedown of ChipMixer, a darknet cryptocurrency mixing service responsible for laundering more than $3 billion worth of cryptocurrency, between 2017 and 2023, in furtherance of, among other activities, ransomware and other hacking schemes. Just one month later, DOJ announced together with international partners the takedown of Genesis Marketplace, which advertised and sold packages of account access credentials – such as usernames and passwords for email, bank accounts, and social media – that had been stolen from malware-infected computers around the world. Access markets like Genesis are key enablers of ransomware.

The 2021 RTF report also called for government-to-government cooperation to establish an "international coalition to combat ransomware criminals" **(Action 1.1.2)**, and the creation of a "global network of ransomware investigation hubs" **(Action 1.1.3)** to help deter cybercriminals, especially by addressing safe havens. In addition to investigative work, Government-led efforts that align with these recommendations, including through the Counter Ransomware Initiative (CRI) are bearing fruit. Australia launched an International Counter Ransomware Task Force in January 2023, for example, to streamline collaboration with CRI member governments. National cybersecurity strategies, as well as ransomware-specific national strategies such as Singapore's Inter-Agency Counter Ransomware Task Force (CRTF), also underscore the importance of addressing ransomware through collaboration across borders and display national governments' commitments to working with partners to address the challenge.

This year, drawing from lessons learned in designing the Ransomware Task Force, the IST cyber team is working to stand up a series of global conversations on implementing the RTF recommendations in specific national contexts, with an emphasis on engaging with Latin American countries. This is especially important given reports that cybercrime is increasing across targets in LATAM countries amid the resource constraints faced by many in the region **(Action 1.3.2)**. Further, leaders continue to prioritize ransomware in their public international engagements, such as the Quad Foreign Ministers' Statement on Ransomware in late 2022.

Increasing Reporting and Information Sharing

To effectively combat any threat, it is necessary to understand it. Building a complete picture of the ransomware threat is complex given its novelty and the siloed nature of the information environment. As highlighted in the section above, public-private partnerships are critical to mitigating this threat, in large part because each sector has access to information that forms a piece of the puzzle. A richer information environment will help clarify the sources of trends we are identifying. For example, a report from Coveware indicates that companies paying ransom demands fell from 85% in Q1 2019 to 37% in Q4 2022. It could be that this decline is the result of recent sanctions against ransomware actors and cryptocurrency entities, together with improved victim cybersecurity. It could also be that these numbers reflect underreporting. Regardless, CrowdStrike reports that in 2023, adversaries are doubling down on stolen credentials, with a 112% year-over-year increase in advertisements for access-broker services. It is thus vital that the community combating ransomware remain vigilant against the threat.

Increasing cyber incident reporting and reciprocal information sharing, including through more proactive government dissemination, will help complete the picture of the ransomware threat, and provide potential pathways to mitigate it. We welcome improved information sharing between the U.S. government and the private sector **(Action 2.3.1)**, especially by sharing tactical reports with relevant technical information to support public defense and response. Still, as noted last year, it will take time for these measures to take effect. In the near term, it is important to encourage voluntary sharing, both amongst key stakeholders in the ecosystem and between them and governments. IST's work to map the ransomware payment ecosystem seeks to support such voluntary sharing and collective action.

The 2021 RTF report also called for a standard format for ransomware incident reporting **(Action 4.2.2)**, and highlighted the importance of increased reporting to better understand and mitigate the ransomware threat. The U.S. government's commitment to CIRCIA's implementation, and the SEC's proposal to require public companies to report cyber incidents indicates an ongoing commitment to strengthening reporting. Similar legislation has been either brought into force or introduced in a number of countries, most notably the reporting provisions included in the EU NIS-2 Directive.[3] Last fall, IST and the Cyber Threat Alliance (CTA) released the *Cyber Incident Reporting Framework: Global Edition*, which outlines best practices for incident reporting in terms that can be adapted by any government. A key observation about these efforts is that to scale and share information closer to real time, myriad reporting requirements should be harmonized to the extent possible.

Reducing Cryptocurrency-Associated Risks

Ransomware is a financially motivated crime. Cryptocurrency forms the backbone of ransomware's profitability by allowing threat actors to obfuscate their connection to illicit proceeds. Stakeholders in the cryptocurrency ecosystem are reducing associated risks of illicit use. In the 2021 RTF report, we urged cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws **(Action 2.1.2)**. As cryptocurrency comes under fire in the wake of events like the late 2022 FTX scandal, governments continue work to enforce know-your-customer compliance and have issued sanctions against cryptocurrency exchanges and mixers like Genesis Market. There is also ongoing consultation under the Financial Action Task Force (FATF) focused on virtual assets.

The 2021 RTF report also emphasized the importance of centralizing expertise in cryptocurrency seizure and scaling criminal seizure processes **(Action 2.1.4)** and incentivizing voluntary information sharing between cryptocurrency entities and law enforcement **(Action 2.1.3)**. A March 2023 FATF report urges governments to build on and leverage existing international cooperation mechanisms and to "develop the necessary skills and tools to quickly collect key information, trace the nearly instantaneous financial transactions and recover virtual assets before they dissipate." The Justice Department's National Cryptocurrency Enforcement Team is well suited for this centralized role, and an April 2023 Treasury report assessing existing risks posed by decentralized finance indicates an ongoing U.S. government effort to reduce cryptocurrency-associated risks. This effort encompasses sanctions such as that targeting the Russian-based Trickbot gang and other designations like the FinCEN statement identifying Bitzlato, a virtual currency exchange, as a "primary laundering concern."

While the impact of these developments is just beginning to show given their recent implementation, efforts to decrease risk will undoubtedly create friction for ransomware actors

[3] The NIS-2 Directive, including discussions of the reporting requirement, entered into force in January 2023 and seeks to harmonize reporting requirements across European Union states: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

seeking to make a profit using these entities. The IST cyber team continues their work to map the ransomware payment ecosystem and identify potential disruptive opportunities through enhanced information sharing, policy recommendations, and other avenues. By mid-2023, we expect to release the results of a mini-pilot, where members of the IST cyber team mapped evidence of ransomware actor tactics, techniques, and procedures over the theoretical map to identify tools and services commonly leveraged by adversaries to carry out attacks.

The Year Ahead: What to Expect?

In the next year, we plan to continue our efforts and galvanize cross-sector work, especially in creating a complete picture of the ransomware threat through data collection and sharing, improving baseline cybersecurity across the ecosystem, and analyzing existing incentive structures.

Ransomware Data: An Incomplete Picture

We are encouraged to see increased data sharing between the public and private sectors and among governments. However, factors like incomplete cyber incident reporting indicate that we still do not have a complete understanding of the scale and scope of this threat. As the ecosystem evolves, it is critical that governments continue to collect and process incident data, work to create target decks of ransomware developers, criminal affiliates, and ransomware variants **(Action 2.3.2)**, and share information with relevant stakeholders in a timely manner.

To supplement incident-specific data, we hope that private sector entities and partner governments will aid in building a clear picture of the threat. This year, we encourage the development of new levers for voluntary sharing of cryptocurrency payment indicators **(Action 2.1.1)** and increased incentives for voluntary information sharing between cryptocurrency entities and law enforcement **(Action 2.1.3)**. Further, we urge governments to create a global network of ransomware investigation hubs **(Action 1.1.3)** to ensure the world addresses this threat as it continues to evolve across the globe.

Improving Baseline Cybersecurity Across the Ecosystem

In last year's report *The Ransomware Task Force: One Year On*, the authors highlighted that "adoption of preparation best practices continues to be slow, particularly among small to medium sized businesses." While governments continue to encourage the adoption of baseline cybersecurity measures for all organizations, more can be done.

The 2021 RTF report recommended that governments highlight available Internet resources to decrease confusion and complexity **(Action 3.1.3)**, run nationwide government-backed awareness campaigns and tabletop exercises **(Action 3.2.2)**, and require local governments and managed service providers to adopt and provide baseline security measures **(Actions 3.3.2; 3.3.3)**. Our analysis indicates that progress has been made in all of these areas. For example, resources like CISA's stopransomware.gov, and NIST's ransomware profile for the Cybersecurity Framework all provide guidance on critical cybersecurity capabilities, especially for small- and medium-sized businesses. However, substantial work remains to improve baseline cybersecurity across all sectors.

Governments are not the only lever for improving baseline cybersecurity. While cyber insurers and reinsurers work to distribute the risk posed by threats like ransomware, they can play a larger role in incentivizing better security by their insureds. By using a tool like the Ransomware Task Force's *Blueprint for Ransomware Defense* to reevaluate underwriting standards, cyber insurers can increase the baseline cybersecurity of the organizations they ensure, thereby making them less vulnerable to attacks and saving money in the long run.

Reexamining Incentive Structures

Ransomware will continue to proliferate as long as systems remain vulnerable to attack and ransomware actors can profit from their crimes. While the 2021 RTF report did not advocate for a ransom payment ban, there are a number of intermediate steps that can be taken to disincentive ransom payments against those most vulnerable to an attack: small- and medium-sized organizations and critical infrastructure entities.

First, many organizations hit with ransomware attacks are small and medium-sized; they are often uninsured and lack the technical personnel to understand the attack itself or respond appropriately. To combat this, the Task Force recommended that the U.S. government investigate the use of tax breaks as an incentive for organizations to adopt secure IT services **(Action 3.4.5)**. The National Cybersecurity Strategy identifies tax structures and other incentives as priorities toward improving the nation's overall cybersecurity. The RTF also recommended that the U.S. government consider alleviating fines for critical infrastructure entities that align with the ransomware framework **(Action 3.4.4)**. We are optimistic that the strategy's implementation will spur informed discussions about these and other tools the government can leverage in this fight.

By shifting existing incentive structures, especially for small- and medium-sized enterprises, organizations will be able to do more to strengthen their cybersecurity before an attack and will be better able to make informed decisions about whether or not to pay if they are ransomed.

It may be telling that there has been no known progress to create ransomware emergency response authorities **(Action 4.1.1)** to help victims make informed decisions in their time of crisis. To further this goal, the 2021 RTF report recommended that stakeholders develop a standard cost-benefit analysis matrix **(Action 4.3.3)** and that the U.S. government require that organizations conduct a cost-benefit assessment and review alternatives before making ransom payments **(Actions 4.3.1; 4.3.2)**. As CIRCIA and other reporting requirements begin to mature, we hope that the data obtained as a result will inform and spark discussion around these lagging recommendations.

Overall, as with last year, we remain optimistic that stakeholders will persist in the fight to combat ransomware. Progress improved significantly over the past year, and when combined with progress in the first year, these collective acts should begin to pay higher dividends in terms of reducing the impact of ransomware incidents as well as bringing additional, global stakeholders into this effort. In the coming year we expect to gain even further ground and continue to build the coalition combating ransomware.

Appendix:

Status of RTF Recommendations by Specific Objective

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**

INSTITUTE FOR SECURITY AND TECHNOLOGY

www.securityandtechnology.org

info@securityandtechnology.org