PUBLIC PRIVATE PARTNERSHIPS TO COMBAT RANSOMWARE

AN INQUIRY INTO THREE CASE STUDIES AND BEST PRACTICES

ELIZABETH VISH

GEORGEANELA FLORES BUSTAMANTE

MARCH 2024

Public Private Partnerships to Combat Ransomware: An Inquiry into three case studies and best practices

March 2024

Authors: Elizabeth Vish, Georgeanela Flores Bustamante
Design: Lillian Ilsley-Greene

Cover text taken from a ransom note sent to a victim in 2023.

Printed in the United States of America

GFCE IST

About the Institute for Security and Technology

As new technologies present humanity with unprecedented capabilities, they can also pose unimagined risks to global security. The Institute for Security and Technology's (IST) mission is to bridge gaps between technology and policy leaders to help solve these emerging security problems together. Uniquely situated on the West Coast with deep ties to Washington, DC, we have the access and relationships to unite the best experts, at the right time, using the most powerful mechanisms.

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

IST aims to forge crucial connections across industry, civil society, and government to solve emerging security risks before they make deleterious real-world impact. By leveraging our expertise and engaging our networks, we offer a unique problem-solving approach with a proven track record.

Acknowledgments

The Institute for Security and Technology (IST) conducted this research with the support of the Global Forum for Cyber Expertise (GFCE), with funding from the Governments of Spain and the United States.

IST executed this research independently, in line with IST's Intellectual Independence Policy, and all conclusions belong to IST. They do not necessarily represent the views of the Government of Spain, the Government of the United States, the GFCE members and partners, or Europol's European Cybercrime Centre (EC3).

We would like to thank the team members at Europol's EC3 and at the Cybersecurity and Infrastructure Agency (CISA) for their time and contributions to this research, and to those individuals who were interviewed for this research. We also thank Patryk Pawlak, who provided research methodology insights and an independent review of the Ransomware Task Force (RTF) case study.

IST would also like to acknowledge the work of the numerous government officials, private sector representatives, and NGOs that have dedicated time and effort to these three examples of public-private partnership. Their engagement is the driving force that makes these collaborations possible. We dedicate this research to all of those involved in building and sustaining public-private partnerships worldwide, particularly those who continue to seek to build these bridges despite seemingly insurmountable gaps between the private and the public sectors.

A note from the authors

We are excited to present this research report on public-private partnerships (PPPs) to combat ransomware. This report reveals the characteristics of three distinct joint efforts. Our intention is for this research to serve as a guide for governments seeking to initiate or improve such partnerships. PPPs are crucial in mitigating ransomware, and we stress the importance of sustaining them as they play an integral role in securing cyberspace.

However, we recognize that the case studies we highlight represent only a fraction of the collective efforts aimed at countering ransomware. The fight against this cyber threat is global, and therefore, approaches to combating it should transcend borders. This entails considering the varying levels of resources available to different countries. As a result, we encourage actively fostering inclusive, collaborative partnerships—domestic, national, regional, and global—to mitigate the impact of ransomware worldwide.

List of abbreviations

CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
CISA	Cybersecurity and Infrastructure Security Agency
EC3	European Cybercrime Centre
JCDC	Joint Cyber Defense Collaborative
LEAs	Law Enforcement Agencies
LEOs	Law Enforcement Officers
PPPs	Public-private partnerships
RTF	Ransomware Task Force
SMEs	Small and medium-sized enterprises
TLP	Traffic Light Protocol

Table of Contents

Executive Summary

This research report examines three existing public-private partnerships to combat ransomware: Europol's European Cybercrime Centre (EC3), the United States Joint Cyber Defense Collaborative (JCDC), and the Institute for Security and Technology's Ransomware Task Force (RTF). In selecting these cases, our goal was to highlight three separate elements of the effort to combat ransomware: criminally focused prosecution and disruption, operational collaboration, and policy measures. Additionally, each model is in different stages of development, with EC3 operating for a decade, and the RTF and the JCDC having launched in late-2020 and 2021 respectively.

This report utilizes these case studies to determine the characteristics of collaboration that make the partnership model successful in mitigating ransomware, as well as identifying the various challenges each faces. Therefore, our main guiding research questions included:

» How do these specific public-private partnerships to combat ransomware operate?

» What principles underlie existing partnerships that can be applied to other contexts and applications?

Case-Specific Research Findings

EC3

Our research into EC3 reveals four formal means of collaboration with the private sector. These include formal information sharing agreements, sector-specific advisory groups, the No More Ransom Project, and joint trainings on issues like open-source intelligence. EC3 excels at engaging industry partners, who commit valuable resources and actively participate in the partnership. We attribute this success to the EC3 staff's understanding of the importance of fostering relationships at the individual level and gradually building a trusted network. However, the EC3's success in fostering partnership may not be replicable across contexts. One significant insight from this case study is that the EC3 relies on substantial resources, including funding and personnel from EU member states, to execute both regional and,

at times, global cybercrime investigations.[1] A critical resource that makes EC3 successful is the participation of law enforcement personnel with deep understanding of cybercrime investigation—something achieved through drawing from Europol's member states. Through a robust collaboration process and the allocation of substantial resources and personnel, Europol achieves excellent results in its cybercrime collaboration with the private sector.

JCDC

JCDC, situated within the U.S. Cybersecurity and Infrastructure Security Agency (CISA),[2] actively organizes coordination efforts across three core areas: products, planning for response and recovery from cyber incidents, and operational collaboration. This report identifies five ways JCDC engages with the private sector, including: formal information sharing agreements, conducting analytic exchanges, coordinating on cyber threat alerts and advisory development, forming actor-specific action groups, and utilizing communication channels such as Slack for real-time information sharing. Two key aspects contributing to JCDC's effectiveness are that CISA leadership recognizes that the private sector holds valuable information about ransomware/cyber threats and acknowledges the vital need for this partnership. However, JCDC grapples with bureaucratic and institutional challenges within the U.S. government's multifaceted approach to cybersecurity collaboration, leading to potential confusion among JCDC participants and hampering information sharing and coordination efforts.

RTF

The RTF, a coalition-led collaboration, distinguishes itself from our other two case studies by being led by a civil society organization. Key collaborative elements involve the RTF's steering committee and co-chairs representing civil society, the technical community, and for-profit organizations. Additionally, the RTF utilizes various lines of effort, including working groups, to address specific issues within the ransomware ecosystem. The collaboration's success is attributed to the RTF's ability to provide clear and focused policy recommendations, leveraging the expertise of its leaders with a range of current and prior experience in policy making across the public and private sectors. With a strong understanding of government processes, the RTF's members frame policy suggestions in a manner conducive to government responsiveness. A challenge to replicating the RTF success, however, is the integral role that civil society actors played. The RTF relies on the organizing capacity of civil

1 The European Parliament and the Council of the EU decide Europol's budget "based on proposals by the European Commission and the Europol Management Board." For more information please see: "Finance & Budget | Europol," Europol, accessed February 13, 2024, https://www.europol.europa.eu/about-europol/finance-budget.

2 CISA sits within the U.S. Department of Homeland Security.

society and volunteerism, drawing on a philanthropic culture within the United States that may not apply in all national contexts.

Best Practices and Practical Recommendations

This report articulates global best practices and lessons learned from our case studies into four key themes. We highlight that successful public-private partnerships to combat ransomware should:

- Include a relevant and tailored range of stakeholders
- Catalyze effective information sharing
- Build trust through clear expectations and person-to-person collaboration
- Learn to navigate practical hurdles within the partnership

As a guide for future initiatives, this report concludes with a brief step-by-step guide on how to establish a partnership to mitigate ransomware and other cyber threats. The steps are:

1. Define the goals of the collaboration
2. Identify key stakeholders and gauge their interest
3. Establish the ground rules for the partnership
4. Start with trust-building practices
5. Look for opportunities to achieve progress
6. Continue to refine the protocols, convening methods, and the overall structure/goals of the partnership as needed

Introduction

Ransomware threatens everything from government IT systems and critical infrastructure operators, to health care systems and small businesses. Stopping the flow of ransomware attacks requires a whole-of-society approach. Governments and the private sector alike have highlighted the need to enhance collaboration between government, law enforcement, and the private sector in order to effectively combat ransomware. However, many of those joint efforts struggle to achieve traction. This research seeks to provide insights into how three cases of public-private collaboration to combat cybercrime operate, and to learn lessons from their efforts.

What is ransomware?

Ransomware is a pervasive and highly destructive form of cybercrime with tangible and severe repercussions. Its reach extends across critical sectors, including hospitals, educational institutions, municipal administrations, and vital public infrastructure. Malicious actors exploit vulnerabilities in network security, holding organizations' digital assets hostage with the primary objective of financial extortion.

Ransomware is a type of malware that renders a victim's files, data, or computer systems as a whole inaccessible until a ransom is paid, often in cryptocurrency. Ransomware attacks may leave individuals, businesses, nonprofits, and governments grappling with compromised data and disrupted operations. Ransomware utilizes asymmetric encryption, generating a unique pair of keys for the attacker and victim.[3] The private key, necessary for decryption, is stored on the attacker's server, and victims are often informed that the private key will be released to them only after the ransom has been paid.[4] Ransomware attacks also can include an additional element of threat to expose data held by the ransomware criminals unless a further ransom is paid, sometimes known as "double extortion."

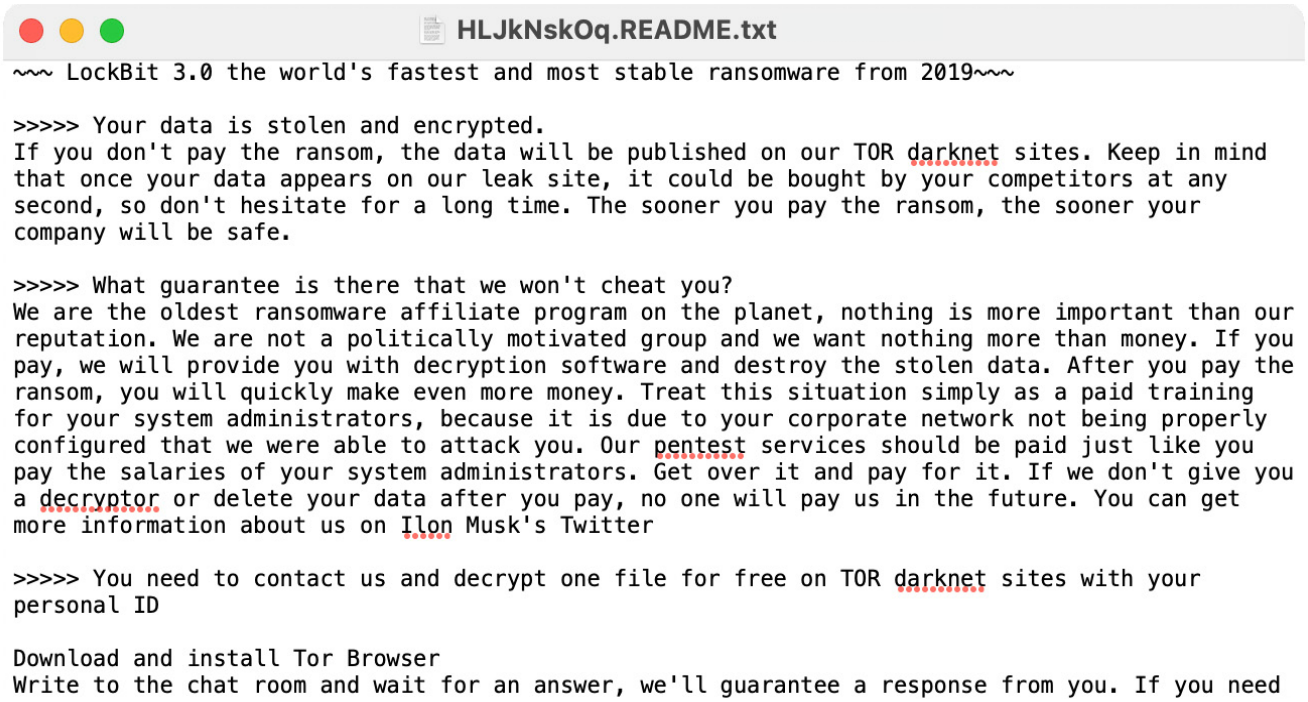
The proliferation of ransomware takes place through various channels, involving the exploitation of vulnerabilities in systems and the use of social engineering tactics. For example, criminals commonly use "phishing" emails to deceive employees within an organization, tricking them into opening attachments that activate the malware and

3 "What Is Ransomware?" Trellix, accessed February 7, 2024, https://www.trellix.com/security-awareness/ransomware/what-is-ransomware/.

4 "What Is Ransomware?" Trellix.

subsequently infect their networks. Once activated, the malware establishes a connection to a command-and-control server, enabling criminals to laterally move across networks and encrypt and/or exfiltrate the organization's data.

Because ransomware can paralyze digital systems, its consequences extend beyond monetary considerations, encompassing the erosion of public trust and confidence in the digital landscape.



HLJkNskOq.README.txt

```
~~~ LockBit 3.0 the world's fastest and most stable ransomware from 2019~~~

>>>>> Your data is stolen and encrypted.
If you don't pay the ransom, the data will be published on our TOR darknet sites. Keep in mind
that once your data appears on our leak site, it could be bought by your competitors at any
second, so don't hesitate for a long time. The sooner you pay the ransom, the sooner your
company will be safe.

>>>>> What guarantee is there that we won't cheat you?
We are the oldest ransomware affiliate program on the planet, nothing is more important than our
reputation. We are not a politically motivated group and we want nothing more than money. If you
pay, we will provide you with decryption software and destroy the stolen data. After you pay the
ransom, you will quickly make even more money. Treat this situation simply as a paid training
for your system administrators, because it is due to your corporate network not being properly
configured that we were able to attack you. Our pentest services should be paid just like you
pay the salaries of your system administrators. Get over it and pay for it. If we don't give you
a decryptor or delete your data after you pay, no one will pay us in the future. You can get
more information about us on Ilon Musk's Twitter

>>>>> You need to contact us and decrypt one file for free on TOR darknet sites with your
personal ID

Download and install Tor Browser
Write to the chat room and wait for an answer, we'll guarantee a response from you. If you need
```

A ransom note from a victim in 2023.

Why is ransomware a global threat?

Ransomware's global reach is rooted in the interconnectedness of today's digital landscape, where criminals can infiltrate and encrypt systems in other countries and hemispheres. Cybercriminals rely on lax law enforcement efforts in safe havens, or on the fact that law enforcement officials are overwhelmed in certain countries, enabling them to operate without impunity and evade prosecution. Many demand to be paid in cryptocurrency, which provides them with a mechanism to avoid the traditional financial system, offering a way to escape anti-money laundering oversight and best practices.

Ransomware is a severe threat because its impacts go beyond a temporary financial burden. An attack can cause substantial harm by taking critical systems offline and halting business operations. As noted in the RTF's 2021 report: "the costs of ransomware go far beyond the ransom payments themselves. Cybercrime is typically seen as a white-collar crime, but while

ransomware is profit-driven and 'non-violent' in the traditional sense, that has not stopped ransomware attackers from routinely imperiling lives."[5] Attacks on critical infrastructure disrupt essential functions such as healthcare services, energy provision, education, food production, and transportation. As such, many governments understand that ransomware poses a threat not only to economic vitality, but to the effective functioning of a society. This means that ransomware rises to the level of a national security threat.

Merrick Garland delivers remarks at the 2023 International Counter Ransomware Initiative Summit.
Photo credit: U.S. Department of Justice, https://www.justice.gov/opa/pr/readout-justice-department-hosting-first-day-2023-international-counter-ransomware.

"Governments recognize the need for urgent action, common priorities, and complementary efforts to reduce the risk of ransomware."

- Joint Statement of the Ministers and Representatives from the Counter Ransomware Initiative Meeting, October 2021 [6]

5 "Ransomware Task Force (RTF) Combating the Ransomware Threat With a Cross-Sector Approach," Institute for Security and Technology, accessed February 8, 2024, https://securityandtechnology.org/ransomwaretaskforce/.

6 White House, "Joint Statement of the Ministers and Representatives From the Counter Ransomware Initiative Meeting October 2021," The White House, 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/.

Why is public-private collaboration critical to mitigating the threat of ransomware?

Ransomware has become too large of a threat for any one entity to address. The scale and magnitude of this challenge urgently demands coordinated global action.

Government, private industry, and civil society can each play a role in addressing the threat. From a government perspective, partnering with the private sector can provide substantial benefits. This includes access to resources and expertise, a broader understanding of threats, and collaboration to exchange information that can lead to better defenses and disruption efforts against ransomware criminals.

Many private sector entities, including small and medium-sized enterprises (SMEs), find themselves targeted by ransomware attacks. Their firsthand experiences as victims—when disclosed—provides invaluable insights into the evolving tactics of cybercriminals. These insights contribute to the development of more resilient cybersecurity strategies that reflect the adaptive nature of ransomware threats. Additionally, ransomware victims are often customers of cybersecurity companies and as a result, these companies can have detailed information about incidents that have occurred.

Many governments have expressed a desire to collaborate with the private sector to address this threat, and have tried to set up collaboration with nonprofits, the technical community, and industry representatives. However, cooperation can be challenging. Sharing information can make non-government entities feel vulnerable to regulatory action or "naming and shaming." Furthermore, entities involved in cybersecurity and combating cybercrime, many of whom operate on a limited budget or with insufficient resources, often struggle to have enough bandwidth to thoughtfully and deliberately build out effective collaboration. This research seeks to help catalyze this collaboration through describing how specific models work and outlining global best practices.

History of the Project

In 2021, the U.S. government launched the Counter Ransomware Initiative (CRI) to bring together governments from across the globe to collaborate in the fight against ransomware.[7] During the second global summit of the CRI in 2022, the governments of the United States

7 To see a list of CRI members as of November 2023, please see: "International Counter Ransomware Initiative 2023 Joint Statement," The White House, November 2, 2023, https://www.whitehouse.gov/briefing-room/statements-releases/2023/11/01/international-counter-ransomware-initiative-2023-joint-statement/.

and Spain announced that they would fund the creation of a "capacity building tool to help countries utilize public-private partnerships to mitigate ransomware."[8] Working with the Global Forum on Cyber Expertise, the world's premier multistakeholder forum focused on cyber capacity building coordination, the Institute for Security and Technology (IST) conducted this research with the primary goals of understanding how effective counter-ransomware collaboration operates and explaining best practices in a way that is actionable for CRI member states.

Research Methodology

IST started the research process by conducting desk research to establish a foundational understanding of the background and context of each case study. Subsequently, we conducted interviews with diverse stakeholders from the public, private, and civil society sectors from September 2023 to January 2024. This approach enabled us to gather insights from a range of perspectives, expanding the breadth of our research.

The writing process was iterative, incorporating valuable feedback from the implementers of each collaboration featured in a case study. As IST convened the RTF, we worked with an independent reviewer to audit our RTF case study and provide third-party feedback on our methodology for this section.[9] We also informed individuals interviewed for the RTF case study that they could share their perspectives directly with the independent reviewer, ensuring confidentiality if they wished to keep certain insights anonymous from our team. Lastly, a draft of this report was reviewed by members of the GFCE and the persons interviewed in our initial research.

Why these three case studies?

This research report investigates three existing public-private partnerships at the forefront of the battle against ransomware: Europol's European Cybercrime Centre (EC3), the United States Joint Cyber Defense Collaborative (JCDC), and the Institute for Security and Technology's Ransomware Task Force (RTF).[10] These case studies focus on three different elements of combating ransomware: law enforcement and crime-focused collaboration through EC3; cybersecurity-focused collaboration, led by the U.S. national civilian

8 "International Counter-Ransomware Initiative 2022: Joint Statement," The White House, November 1, 2022, https://www.whitehouse.gov/briefing-room/statements-releases/2022/11/01/fact-sheet-the-second-international-counter-ransomware-initiative-summit/.

9 The authors of this report work for the Institute for Security and Technology (IST).

10 The selection of the RTF as one of the cases for this research was done in collaboration with the governments of Spain and the United States and the Global Forum for Cyber Expertise as well as an open call for input from GFCE members. IST's intellectual independence policy can be found here: https://securityandtechnology.org/intellectual-independence-policy/.

cybersecurity agency through the JCDC; and policy-focused measures led by civil society and the technical community in the RTF. The following three case studies emphasize that ransomware mitigation efforts are multifaceted, showcasing different dimensions and developmental trajectories within the realm of public-private partnerships dedicated to countering ransomware.

Ransomware Incident Response: The collaboration between Spain and Costa Rica

While this report primarily addresses public-private partnerships in combating ransomware, government-to-government cooperation is also critical. Therefore, this spotlight provides a brief discussion of one specific collaboration: the 2022 counter-ransomware collaboration between Spain and Costa Rica. There have been other instances of collaboration between national governments to address ransomware incidents of national security concern.[11] We encourage governments to engage in such collaborations whenever possible.

In 2022, the Costa Rican government suffered two ransomware attacks. In response, Costa Rica's National Intelligence and Security Directorate (DIS, by its Spanish acronym) initially requested support from Spain's National Intelligence Center. Spain and Costa Rica had pre-existing cybersecurity cooperation agreements that were leveraged to initiate assistance. These pre-existing engagements helped lay the groundwork for swift collaboration in response to Costa Rica's ransomware incidents. Spain's National Cryptologic Center (CCN-CERT) dispatched a team of technical experts to Costa Rica, which included members from the private sector. The team provided technical support, conducting reverse engineering analysis of the malware and equipping Costa Rica with a ransomware-thwarting tool.[12] Additionally, this team collaborated with Costa Rica's DIS and Ministry of Science, Innovation, Technology, and Telecommunications (MICITT, by its Spanish acronym). They held joint meetings specifically throughout the first ransomware incident.

Costa Rica and Spain maintain ongoing communication in the aftermath of the ransomware incidents. Specifically, Spanish authorities have ongoing communication lines with Costa Rica's DIS, MICITT, and Computer Incident Response Team (CSIRT-CR). Additionally, Costa Rica participates in conferences held by Spain in Europe. These interactions ensure open communication channels, foster trust, and aid in cyber capacity building.

This case demonstrates the value of establishing collaborations in advance of cybersecurity incidents of national security concern, which builds trust in advance of an emergency request. These channels made it far less difficult to initiate the formal request for emergency assistance.

11 For example, to read about the cooperation between Vanuatu and Australia, please see: Alexander Martin, "Australia and Vanuatu Sign Defense and Cybersecurity Pact," The Record, December 12, 2022, accessed March 19, 2024, https://therecord.media/australia-and-vanuatu-sign-defense-and-cybersecurity-pact.

12 Eugenia Lostri and Georgia Wood, "The Role of International Assistance in Cyber Incident Response," Lawfare, March 30, 2023, accessed March 19, 2024, https://www.lawfaremedia.org/article/role-international-assistance-cyber-incident-response.

Europol's European Cybercrime Centre

Europol is the European Union's agency for law enforcement cooperation.[13] As such, the agency actively supports investigations initiated by EU member states, with a focus on cases that require coordination across various jurisdictions, including jurisdictions outside the EU.[14] Additionally, Europol has the "legal mandate to cooperate with law enforcement agencies (LEAs) across Europe."[15] In 2013, Europol established the European Cyber Crime Centre (EC3) to bolster the EU's collective response to cybercrime.[16] Its creation marked a significant step forward in safeguarding European citizens, businesses, and governments from the ever-evolving landscape of cybercrime. EC3 operates as a dedicated hub of expertise, focusing on addressing cyber threats from multiple angles. Its versatile role includes providing operational, strategic, analytical, and forensic support for member states' investigations.[17] This encompasses the Expertise and Stakeholder Management Unit, which builds crucial partnerships, the Digital Support Unit, which provides real-time forensic support, and the Operational Teams (Analysis Projects), which investigate various cybercrimes. Central to this paper's research question, EC3 employs public-private partnerships to aid it in efforts to combat ransomware. This first case study explores how EC3's position as a cybercrime center has contributed to the fight against ransomware through these partnerships.

13 Europol was formed in 1995 through the signing of the Europol Convention, and attained full EU Agency status in 2009 under the Lisbon Treaty. In May 2017, Europol's new regulation facilitated the agency's capacity to develop specialized units for addressing diverse and emerging threats. For more information about Europol's legal framework, please see: https://www.europol.europa.eu/cms/sites/default/files/documents/celex_32016r0794_en_txt.pdf.

14 It should be noted that Europol officers never arrest citizens. For more information see: "About Europol | Europol," Europol, accessed October 17, 2023, https://www.europol.europa.eu/about-europol.

15 "About Europol | Europol," Europol.

16 The Joint Cybercrime Action Taskforce (J-CAT) sits within EC3 and contributes to mitigating cybercrime both within and beyond the EU. For more information about this task force, please see: "Joint Cybercrime Action Taskforce (J-CAT) | Europol," Europol, accessed March 1, 2024, https://www.europol.europa.eu/operations-services-and-innovation/services-support/joint-cybercrime-action-taskforce.

17 "European Cybercrime Centre - EC3 | Europol," Europol, accessed October 18, 2023, https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

Assistance to Law Enforcement on Combating Cybercrime

Since the capacity of law enforcement officials to investigate cybercrime is one serious obstacle to public-private collaboration, multiple entities offer cybercrime capacity building to law enforcement officials and others within government who support counter-cybercrime goals. The GFCE engages on counter-cybercrime efforts through the multistakeholder Working Group C,[18] and also shares information about cybercrime capacity building on the Cybil Portal, the GFCE's knowledge portal for cyber capacity building, available at cybilportal.org. Cybil highlights over 200 projects that include cybercrime as a key theme, ranging from missions within the European Union that focus on cybercrime legislation harmonization, to public awareness campaigns to help citizens not be fooled by cyber criminals, to private company assistance for national governments.

One key program that the authors of this report wish to highlight is the Council of Europe's Cybercrime Programme Office (C-PROC). C-PROC works to strengthen criminal justice capacities to counter the challenges of cybercrime and electronic evidence. This assistance is given in line with the Budapest Convention on Cybercrime and its Protocols, and since 2014 has supported more than 2,100 activities in the form of workshops, legislative advice, and trainings, benefitting over 130 countries. C-PROC's activities are focused on strengthening domestic criminal law in line with the Budapest Convention on Cybercrime, and its Second Protocol on electronic evidence; capacity building for practitioners, such as domestic simulation exercises on effective data sharing between cybersecurity and cybercrime communities; providing platforms and gatherings for dialogue among practitioners and public-private cooperation, such as the Octopus Conference; and developing materials like Council of Europe's guide for conducting criminal investigations of ransomware attacks. The most comprehensive Council of Europe support is given to those States that are Parties or have been invited to accede to the Budapest Convention.

Public - Private Collaboration Mechanisms

EC3 has four formal means of collaborating directly with the private sector:

Information Sharing, Coordination, and Deconfliction

The regulation that guides Europol's engagement had for a long time prevented the agency from receiving information from private actors, instead requiring data to be passed to Europol by national law enforcement agencies.

18 The GFCE organizes its efforts around five key areas, and convenes working groups on each effort. Working Group C's description can be found here: https://thegfce.org/theme-gfce/cyber-crime/.

However, due to amendments to the Europol Regulation (Regulation (EU) 2016/794) in 2022, Europol is now able to receive data directly from private sector entities. As noted by an interviewee at a global financial institution:

> *"It's super useful, because only around 1% of cases get reported to the police. Additionally, local law enforcement are completely swamped... We have all of this information that we can be sharing with law enforcement agencies [LEAs], and now we can do so directly. We believe that the more [meaningful] data international law enforcement agencies have, the higher the chance of having a real impact on the cybercrime ecosystem."*

To facilitate information sharing, EC3 signs Memorandums of Understanding (MOUs) with various private sector entities. EC3's MOUs act as a commitment to cooperate as much as possible, while respecting public, private, and legal obligations. MOUs do not set mandatory standards for cooperation; rather, they identify common interests and note that the partnership will continue as long as it is beneficial to both parties. Through this mechanism, private industry representatives have shared information regarding items such as criminal intrusion into critical infrastructure and data about virtual assets linked to ransomware actors.

Further, EC3 employs a range of protocols to protect the security and confidentiality of information to assure participants that their information will be appropriately protected. EC3 uses the Europol Information classification levels,[19] but respects the Traffic Light Protocol (TLP) when working with private parties to achieve common understanding regarding the sensitivity of shared information and guide appropriate sharing.[20] Moreover, to facilitate secure data transmission, EC3 relies on Europol's Secure Information Exchange Network Application (SIENA) and PGP-encrypted emails.[21]

In addition to facilitating one-off sharing, these direct exchanges allow Europol and members of the cybersecurity and technical community to directly coordinate their respective counter-crime actions and deconflict their research and other actions they undertake to protect their customers and/or partners. As noted by one representative of a Europe-based cybersecurity company, companies want to ensure that their efforts to protect customers do not inadvertently expose law enforcement investigation methods or current investigator lines of inquiry. The interviewee highlighted that having ongoing communication with LEAs is critical, as it allows for deconfliction at any point in the law enforcement investigatory process, including before an investigation starts.

19 For more information on Europol Information classification levels, please see "Acts Adopted Under Title VI of the EU Treaty" in the Official Journal of the European Union: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:332:0017:0022:EN:PDF.

20 For more information on the Traffic Light Protocol, please see page 22.

21 For more information on the SIENA mailbox system, please see: https://www.europol.europa.eu/operations-services-and-innovation/services-support/information-exchange/secure-information-exchange-network-application-siena.

Advisory Groups

EC3 has established three specialized advisory groups that serve as the primary channel for the agency to engage with the broader private sector. These groups focus on establishing cooperation between law enforcement agencies and entities within three critical areas: Internet security, financial services, and communications providers.

EC3 has a fixed number of seats within these advisory groups, allowing the agency to prioritize entities that have demonstrated their value and continue to actively participate. Membership is reassessed every two years, allowing EC3 to respond to challenges posed by the evolving cybercrime landscape. Private sector partner representatives undergo a rigorous clearance process spanning several months before they are admitted into the advisory groups.

These advisory groups address the evolving landscape of cybercrime trends. Their key aims include the following: assist EC3 in defining priorities within their areas of expertise, update and share all relevant sector-specific information and developments, and "advise EC3 on how to increase the sharing/exchange of information between law enforcement and each sector."[22]

The No More Ransom Project

The No More Ransom Project aims to "help victims of ransomware retrieve their encrypted data without having to pay the criminals."[23] The project's portal began operating in July 2016, with four founding partners: EC3, the National High Tech Crime Unit of the Netherlands' police, Kaspersky Lab, and McAfee.

Partners contribute to No More Ransom in three distinct ways. First, a standing group of founding and associate partners for the No More Ransom project contribute analysis, decryption tools, and support with ongoing engagement in the project. Second, a group of dozens of companies contribute relevant technical solutions, such as a decryption key, when they have them. Third, supporting partners, which include many law enforcement agencies across the globe as well as dozens of private companies and civil society members, assist in informing organizations and businesses about the No More Ransom project.[24]

22 For a list of the private sector partners within each advisory group, please see: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners.

23 "About the Project | The No More Ransom Project," The No More Ransom Project, accessed October 19, 2023, https://www.nomoreransom.org/en/about-the-project.html.

24 "Partners | The No More Ransom Project," The No More Ransom Project, accessed October 25, 2023, https://www.nomoreransom.org/en/partners.html.

Training

Europol also collaborates directly with the private sector through law enforcement officer trainings, during which private sector representatives train officers on topics such as open source intelligence, quantum computing, and evidence gathering practices. When discussing how this training supports the EC3 collaboration, an interviewee from a global financial institution stated: “We always try to bring something to the table, like a case that can help others, to provide an integrated landing site for this collaboration.”

Why does the private sector collaborate through EC3?

Private actors highlighted the following four reasons:

- **To see outcomes in cybercrime cases:** Private sector organizations possess valuable insights into ransomware incidents, such as victim information and cybercriminal tactics. However, they lack the authority and resources to directly pursue cyber criminals through criminal indictments or to impose other consequences, such as implementing sanctions or seizing profits of ransomware attacks. Collaboration with law enforcement agencies allows the private sector to contribute to those efforts and see a tangible impact on criminals.
- **To improve the overall cybersecurity landscape:** Industry partners collaborate with Europol to contribute to regional and global cybersecurity efforts, thereby enhancing online safety. This collaboration involves not only avoiding interference with law enforcement operations, but also supplementing the work that law enforcement agencies undertake to reduce vulnerabilities through information sharing and exchange of best practices.
- **To facilitate information sharing between private sector entities:** Companies value engaging in a non-competitive environment where they can share threat data in a neutral setting that enforces a norm of mutually beneficial information exchange. This practice benefits both their clients, and their internal understanding of the cybercrime landscape.
- **To gain credibility and burnish their brand:** Private sector partners value public recognition and acknowledgement of their efforts as a useful and reliable contributor by the Europol authorities. As noted by a representative from a Europe-based cybersecurity

company, "[working with LEAs] helps to build brand awareness." Partners see public acknowledgement of their progress as showcasing that "we have the ability to help victims out and demonstrate our expertise."

Key Aspects That Drive EC3 Public-Private Partnership Success

» **A commitment to mutual respect and exchange:** Europol understands that it needs contributions from private industry, the technical community, and civil society in order to effectively fight ransomware and cyber threats. Therefore, EC3 has created systems to allow for meaningful exchange that benefit private industry and other participants. This involves a willingness to maintain the partnership's momentum by seeking out new partners on a regular basis and maintaining an openness to collaboration to the fullest extent allowed by policy and the law.

» **Identifying relevant and cooperative partners:** EC3 recognizes the vital importance of cultivating relationships at the individual level within a public-private collaborative and gradually building a trusted network from those foundational connections. As noted by an interviewee, it is critical that partners be willing to share information and commit to "collaborat[ing] in all ways possible." Europol team members regularly meet with new possible partners to discuss their priorities and learn about their work. At the same time, they are extremely selective of partners that they invite into closed door exchanges in order to facilitate trust and open sharing.

» **Managing legal authorities and expectations of actions:** Representatives of private industry who collaborate in EC3's work do so with the understanding that there are things that law enforcement agencies uniquely have the mandate to do. Conversely, there are things they cannot do, such as sharing sensitive details about ongoing investigations. EC3 also makes it clear that sometimes, information shared will not be met with substantial exchange of other relevant information, because ongoing investigations make the information very sensitive.

» **Providing for regular turnover of collaboration:** Since seats in EC3's publicly-facing advisory groups are limited, participants must demonstrate continued value and commitment to exchanging information in order to maintain a seat at the table. This commitment comes in the form of active contributions of intelligence in meetings and the timely creation of reports. While private sector companies commonly engage in initiatives aligned with their interests, Europol's EC3 is able to facilitate collaboration

beyond contributions narrowly tied to industry actors' immediate corporate interests in order to maintain their long-term participation in the effort. EC3 achieves this through requiring robust contributions from everyone into the advisory groups, making it so that organizations have to contribute meaningfully in order to get the benefits of participation.

» **Proactive approach to collaboration/engagement:** A final factor contributing to EC3's success is its proactive approach to staying abreast of what the private sector is sharing publicly about its insights. EC3 achieves this by inviting industry partners to present their findings to Law Enforcement Officers (LEOs) before public dissemination. This approach not only facilitates deconfliction efforts, but also underscores EC3's commitment to maintaining a nuanced understanding of the evolving cyber threat landscape.

Challenges in Collaboration between Europol EC3 and Private Partners

» **Substantial collaboration resources:** The resources required for these robust, cross-jurisdictional, and intense collaborations present a challenge for jurisdictions with lower resource levels. Europol's access to funding and the pooling of expertise from across the EU region facilitates its ability to undertake such collaborations. However, its success depends on governments in the region being willing to provide staff on a medium-term basis and continuing to view this public-private partnership as a valuable endeavor.

» **Delays or limited responses from Europol:** Sharing sensitive information with law enforcement poses a challenge, as companies may experience a prolonged period of silence after sharing, during which they are unaware if or how law enforcement officers have used the information provided. It may be months or years before Europol and other law enforcement officials can tell organizations that the information they shared was critically helpful; public recognition for their efforts may be significantly delayed, or in fact impossible. Companies have to understand that not all information shared will have immediate results, and yet should continue to share information that they see as potentially relevant.

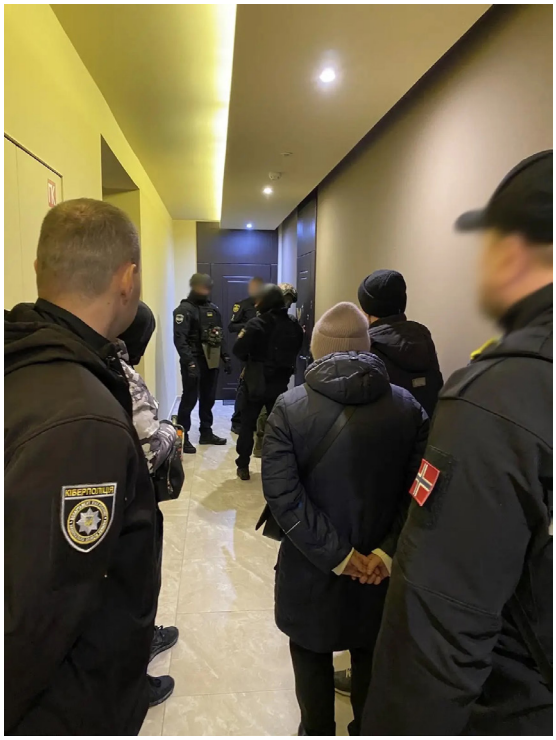
» **Crucial role distinction:** Contributing companies have to understand that EC3's law enforcement mandate means that there may be instances where Europol cannot reciprocate information sharing on an equal basis from law enforcement to private sector partners. This can happen when the information shared by the industry pertains to ongoing investigations, limiting Europol's ability to provide responses and information

sharing to any private sector partners. Industry partners need to understand and accept this limitation while remaining engaged with the partnership.

» **Sustaining trust amid role shifts:** Maintaining collaboration when individuals shift roles is a serious challenge, as much of the trust is built on personal relationships. EC3 has undertaken substantial work to institutionalize collaboration, but there is a level of trust maintenance that needs to continue even if different people are sitting in the chair.

Examples of EC3's Public-Private Cooperation Success

» **Operation Fifth Element:** In November 2023, in a coordinated international law enforcement effort, authorities from Norway, France, Germany, the United States, the Netherlands, Switzerland, and Ukraine, with the support of Europol and Eurojust, successfully dismantled a ransomware group. This group was responsible for attacks in 71 countries. Authorities arrested the 32-year-old ringleader and four accomplices, conducting searches across Ukraine, and overcoming the complexities of the country's conflict with Russia. Bitdefender and other private sector partners contributed decryptors to the No More Ransom project in support of this case.



Operation Fifth Element. *Photo credit: Europol*.

» **Operation HashGuard:** In January 2024, Europol and the National Police of Ukraine worked together with a major cloud service provider to investigate and arrest an individual believed to be the mastermind behind a sophisticated cryptojacking scheme. The arrest came as the result of a year of collaboration between Europol, the Ukrainian authorities, and the cloud provider.

View more examples of Europol's successes.

Global Law Enforcement Cooperation through INTERPOL

Recognizing that Europol's EC3 primarily focuses on investigations initiated by EU member states, and that our following two case studies predominantly center around counter-ransomware and cybersecurity efforts within the United States, we are committed to ensuring a comprehensive understanding of global cybersecurity initiatives. In pursuit of a broader perspective, we have included a brief look into how INTERPOL collaborates with the private sector.

INTERPOL, short for the International Criminal Police Organization, has an extensive network spanning 196 member countries. It enables police forces in member countries to actively share and access data related to crimes and criminals, providing technical and operational support. The organization includes reducing cybercrime among its focus areas.

INTERPOL actively engages in partnerships with organizations and private companies in the information technology, cybersecurity, and financial sectors. Collaborative efforts include information sharing, intelligence analysis, and support for capacity building and training activities. Furthermore, private sector involvement provides valuable insights into the infrastructures and operations of cyber organized crime groups, as well as new and emerging technologies such as artificial intelligence, aiding in an extensive global response to cyber threats.

INTERPOL's partnership process involves a preliminary assessment of a private sector entity's capabilities, followed by a thorough due diligence process to identify and mitigate risks posed by the collaboration. INTERPOL undertakes this step in order to ensure that the private sector's activities and values align with its goals.

View a selection of INTERPOL's success stories in partnering with the private sector to combat ransomware.

The Joint Cyber Defense Collaborative

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) is the "operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience."[25] In 2021, CISA established the Joint Cyber Defense Collaborative (JCDC) to gather, analyze, and share actionable cyber risk information.[26] JCDC, a public-private collaborative, unites a broad spectrum of entities in pursuit of its mission to mitigate cyber threats, including government agencies, industry players, and international cybersecurity organizations.[27] Government participants, such as the Department of Homeland Security, U.S. Cyber Command, the National Security Agency, the Federal Bureau of Investigation (FBI), the Department of Justice, and the Office of the Director of National Intelligence actively engage in this collaboration, and additional agencies are brought in when relevant.[28] Non-government participants include "service providers, infrastructure operators, cybersecurity companies, companies across critical infrastructure sectors, and subject matter experts (SMEs)."[29] Globally, JCDC maintains ongoing collaboration with "over 100 cyber defense organizations or computer emergency response teams (CERTs)."[30]

JCDC collaborates with private sector organizations—both for-profit companies and the technical and research community—in various capacities depending on area of expertise, scope, and capability. Some entities contribute to a specific cyber defense planning effort focused on a particular risk scenario, while others engage by participating in an operational collaboration effort centered on a specific threat or vulnerability.

25 "About CISA | CISA," Cybersecurity and Infrastructure Security Agency CISA, accessed November 29, 2023, https://www.cisa.gov/about.

26 "Joint Cyber Defense Collaborative | CISA," Cybersecurity and Infrastructure Security Agency CISA, accessed November 29, 2023, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative.

27 "JCDC FAQs | CISA," Cybersecurity and Infrastructure Security Agency, accessed November 30, 2023, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-faqs.

28 "JCDC FAQs | CISA," Cybersecurity and Infrastructure Security Agency.

29 "JCDC FAQs | CISA," Cybersecurity and Infrastructure Security Agency.

30 "JCDC FAQs | CISA," Cybersecurity and Infrastructure Security Agency.

CISA organizes its coordination of JCDC into three core areas.

Products: CISA works with JCDC members to produce alerts and advisories that cover emerging threats, general cybersecurity best practices, and ransomware variants and actors. These alerts primarily target public consumption, but also include guidance tailored to specific audiences. Although this effort is dedicated to information sharing within the United States, the information often holds relevance for the wider global cybersecurity community. An example of this work includes efforts such as the July 2023 advisory on Citrix vulnerabilities,[31] which incorporated input from information security company Mandiant and the non-profit Shadowserver Foundation.

Planning: In line with 2021 legislation, CISA's planning team works with JCDC participants to collaboratively create cyber defense strategies for both public and private sectors, including coordinated measures to protect, detect, respond, and recover from cyber incidents.[32] This includes efforts to establish joint priorities with partners through a framework known as the planning agenda.

Operational Collaboration: Under JCDC, representatives from cybersecurity companies, critical infrastructure operators, service providers, and others with key insights into threats and vulnerabilities collaborate with JCDC government participants—as well as state, local, tribal and territorial authorities—to take collective action to reduce cybersecurity threats and vulnerabilities impacting U.S. organizations and the global Internet ecosystem.

Public-Private Collaboration Mechanisms

JCDC has five formal means of collaboration with the private sector:

Actor-Specific Action Groups

JCDC convenes groups to collaborate on specific ransomware actors, with the goal of exchanging relevant information so that government and private actors can connect the dots between specific types of information, such as virtual private networks (VPNs) used by the actors or specific vulnerabilities, tactics, techniques, and procedures used by the actor. In these action groups, CISA selects the actor of focus, and the government and private sector participants share specific information about the actor with the group. In at least one case, the

31 "Threat Actors Exploiting Citrix CVE-2023-3519 to Implant Webshells | CISA," Cybersecurity and Infrastructure Security Agency CISA, July 20, 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-201a.

32 See Section 1715 of the 2021 National Defense Authorization Act for more information: https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf.

government kicked off the conversation by providing the initial round of information, which served to effectively catalyze other members to contribute relevant information as well. These action groups also included opportunities for members to meet in person and get to know each other, building the person-to-person trust that facilitates more effective sharing.

Information Sharing Agreements and Other Formal Agreements

JCDC establishes formal information sharing agreements with private sector partners that leverage the statutory frameworks provided by the Homeland Security Act of 2002, as amended, and the Cybersecurity Information Sharing Act of 2015.[33] Not all private sector partners engage in formal information sharing agreements, reflecting varied levels of partnership involvement and comfort with informality among partners. In certain cases, JCDC may formalize a partnership that has been mutually beneficial over a period of time by introducing a formal partnership agreement. This legal agreement fortifies the mutual commitment to collaboration between CISA and the partner.

JCDC also uses the Traffic Light Protocol (TLP), which interviewees cite as an important element to building trust among stakeholders within the JCDC. JCDC categorizes all alerts and advisories based on the TLP, facilitating clarity for recipients on how to manage the information that they may want to share onward. This intentional categorization streamlines the decision-making process for recipients, indicating whether information should be closely guarded or can be shared with other entities. In turn, JCDC also respects information shared with them that has been designated according to TLP. One interviewee highlighted how this approach reinforces a trusted relationship, assuring entities, victims, and partners sharing information with JCDC that their information will be protected.

33 "Cybersecurity Information Sharing Act of 2015 Procedures and Guidance | CISA," Cybersecurity and Infrastructure Security Agency CISA, October 15, 2021, https://www.cisa.gov/resources-tools/resources/cybersecurity-information-sharing-act-2015-procedures-and-guidance.

What is the Traffic Light Protocol?

The Traffic Light Protocol (TLP) is a method for articulating how to place bounds around sharing potentially sensitive information, devised in an effort to facilitate information sharing and build more effective collaboration. The benefit of the TLP system is that it provides, "a simple and intuitive schema for indicating with whom potentially sensitive information can be shared."[34] From the start, TLP has been a collaborative undertaking: the incident response community developed it, the Forum for Incident Response and Security Teams (FIRST) standardized it and continues to manage it, and the cybersecurity technical community regularly employs it. TLP articulates four information sharing categories, from TLP:CLEAR which can be disseminated broadly, to TLP:RED which cannot be shared beyond the individual recipient. For more information on TLP and how to utilize it, please refer to the FIRST Standard Definitions and Usage Guideline: https://www.first.org/tlp/.

Traffic Light Protocol Guide

TLP:RED

For the eyes and ears of *individual recipients only*, no further disclosure. Sources may use TLP:RED when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

TLP:AMBER + STRICT

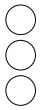
Sharing restricted to the *organization only*. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT.

TLP:AMBER

Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients.

TLP:GREEN

Limited disclosure, recipients can spread this within their *community*. Sources may use TLP:GREEN when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. Note: when "community" is not defined, assume the cybersecurity/defense community.



TLP:CLEAR

Recipients can spread this to the *world*, there is no limit on disclosure. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.

Definitions from FIRST Standard Definitions and Usage Guidelines: https://www.first.org/tlp/

34 For more information about the FIRST Standard Definitions and Usage Guideline, please see: https://www.first.org/tlp/.

Communication Channels

JCDC shares information and ensures ongoing open dialogue through a variety of platforms. Persistent collaboration channels often use Slack, including channels for participants from specific sectors for ongoing collaboration, and channels created for a defined time to work on particular operational issues. Slack comes with the ability to establish smaller channels for operationally sensitive activities. While some of these channels are used to continuously share information, others are periodically dormant and are intended to provide an available platform where participants can immediately convene and collaborate if the need arises. JCDC additionally uses other government-run information sharing platforms like the Homeland Security Information Network (HSIN)[35] and distributed emails for broader, uni-directional information sharing.

Analytic Exchanges

JCDC organizes two annual meetings, referred to as analytic exchanges, which are governed by the Traffic Light Protocol. These meetings are co-delivered by government and industry stakeholders and are attended by a broad range of partners. Beyond sharing technical knowledge, research, and novel tools, these meetings facilitate trust-building through face-to-face interactions and more informal dialogues between stakeholders.

Coordination on Developing Advisories

During CISA's advisory release process, CISA works with JCDC to circulate draft advisories among industry partners with relevant subject matter expertise. JCDC private sector partners are able to contribute insights from their perspectives, in some cases utilizing datasets to potentially enhance advisory accuracy. Furthermore, primary industry partners can review the advisories, providing evidence-based insights that contribute to a more thorough understanding. This collaborative approach helps to ensure accuracy and enables JCDC to ultimately produce more comprehensive reports for the cyber community.

35 The Homeland Security Information Network (HSIN) is the Department of Homeland Security's official system for trusted sharing of Sensitive But Unclassified (SBU) information between federal, state, local, territorial, tribal, international and private sector partners. https://www.dhs.gov/homeland-security-information-network-hsin.

Why Does the Private Sector Collaborate with JCDC?

» **Improving cybersecurity in the United States and globally:** Companies engage with JCDC to have a forum that unites diverse stakeholders around a mission of protecting U.S. critical infrastructure from cybersecurity threats. According to one interviewee, they "just want to get data in the right hands," so that someone can act upon it to make the digital ecosystem more secure. Furthermore, recognizing that industry partners are often mission-driven, being part of an initiative with the capacity to protect national security augments their company mission.

» **Gaining a more nuanced understanding of threat actors**: A representative from a cybersecurity company expressed that the JCDC provides a platform for conversations about disrupting human networks involved in cyber threats. More nuanced discussions on topics such as real-time identification of cybercriminals, rather than solely attributing actions to software, allow for a more comprehensive approach to addressing and countering cybersecurity challenges.

» **Helping to pool expertise:** Collaborative efforts like JCDC allow organizations to pool expertise and connections to counter cyber threats more effectively. Smaller organizations that may not have the same level of resources, sufficient personnel, and/or technical knowledge as extensive as larger enterprises in particular stand to benefit from this collaboration.

Key Aspects that Drive JCDC's Effectiveness

» **Legislative mandate and leadership understanding of the vital need for partnership:** The JCDC was created by legislation written by both political parties in the U.S. legislature, and was created with broad support from the American public.[36] Both CISA leadership and private entities participating in JCDC recognize the essential need for collaboration between government and industry partners. Interviewees who participate in JCDC efforts note that effective information sharing and collaborative operations are vital, because government and industry actors each hold unique insights into cybersecurity threats. Participants also noted a deep desire to continue to enhance the partnership.

36 For more information about JCDC, see Section 1715 of the 2021 National Defense Authorization Act: https://www.congress.gov/116/bills/hr6395/BILLS-116hr6395enr.pdf.

- **Facilitation of information exchange:** As part of the actor-specific action groups, CISA has regularly kicked off collaboration by sharing government-held information first. This highlights a priority for JCDC work: facilitating information exchange between entities that would not normally share information but can do so in this type of neutral forum. For example, two private companies may be business competitors, but each might have information that, if combined, could help protect potential ransomware victims. JCDC provides opportunities for these companies to share this information in a neutral venue.
- **Opportunity for exchange on strategic priorities:** One of JCDC's objectives is to share government priorities for cybersecurity defense with industry and private sector representatives, with the goal of systematically highlighting gaps in critical infrastructure cybersecurity postures. For private sector participants, including sector operators, researchers, and major service providers, participating in JCDC can help them focus government attention on the trends and defense priorities that are coming up in their research or customer/client protection efforts.
- **Desire to address sector-specific needs:** JCDC members have articulated that different sectors have different needs, and that some sectors need more tailored assistance when it comes to mitigating cyber threats. This is especially important in sectors that are known to be targeted repeatedly by cybercriminals, particularly ransomware actors, but are not as well equipped to handle a major cyberattack. For example, in 2023 JCDC focused on the water and wastewater sector, and also the energy sector in collaboration with the Department of Energy. Coordination with relevant Sector Risk Management Agencies is a critical consideration for all of the JCDC's sector based work and deliverables.[37]

Challenges that JCDC Faces in Collaboration between Government and Private Sector

As an effort only in existence since late 2021, JCDC is still working out administrative and logistical difficulties, as well as growing into its mandate. Many of the challenges described are commonly found in the process of standing up new public private partnership initiatives.

- **Building sustainable momentum with stakeholders:** One challenge for JCDC is continuing to engage partners over the long term, particularly as the immediate response following the full-scale Russian invasion of Ukraine in the first half of 2022 faded. Multiple interviewees noted that they saw certain companies push forward

37 A discussion of the role played by Sector Risk Management Agencies can be found here: tps://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/sector-risk-management-agencies.

proactive engagement with the JCDC, but received very little response from CISA, which eroded their company or entity's interest in ongoing participation. They highlighted that government actors must be responding on a regular basis in order for non-government stakeholders to be available when the government has an ask of JCDC members. These interviewees noted that they still want to participate in JCDC, and encouraged CISA representatives to redouble their efforts to engage at a sustainable and regular tempo.

» **Managing information channels:** Ensuring streamlined communication channels without overwhelming stakeholders remains a challenge for JCDC participants. In some cases, participants pointed towards redundant information being shared repeatedly, or information being "recycled" by the government without acknowledgement that it had been contributed by a non-government participant. Two researchers noted that this eroded the usefulness and trust in JCDC practices to both acknowledge and respect partners. It is important to note that not all partners want to be named specifically when sharing information; however, understanding the origin of knowledge and contributions—whether it came from the private or public sector—helps to better contextualize discussions among participants. Logistically, partners also noted that they had fallen out of specific communication efforts, such as "timing out" of Slack channels without clear support on how to get reengaged.

» **Supporting varied capabilities:** JCDC has to be able to provide support to entities with vastly different levels of capabilities when it comes to industry partners. One interviewee pointed out that cybersecurity recommendations made by CISA in collaboration with the JCDC are more easily implemented by large, well-resourced companies than by small and medium enterprises (SMEs).

» **Lack of clear explanations for inclusion and exclusion criteria:** One interviewee emphasized JCDC's challenge in clearly explaining how participants are selected, both at the ongoing level as well as for specific collaborations. While acknowledging that not all actors are relevant to every collaboration, the challenge highlights the need for JCDC to articulate inclusion or exclusion decisions in joint efforts.

» **Measuring indirect impacts:** For activities such as issuing cybersecurity alerts or advisories, it is difficult to know whether private sector entities have implemented the guidance, and if so, to what degree the guidance has led to long-term improvements in those entities' protection from cyber attacks.

» **Addressing institutional and bureaucratic challenges:** While JCDC is a critical priority of CISA and has strong support from many in the cybersecurity community, multiple interviewees pointed to difficulties coordinating between U.S. government partners.

Particularly within specific sectors, interviewees noted that sector-specific government entities had their own information sharing platforms or processes that had more relevant and effective practices; therefore, entities within that sector prioritized participation in sector-specific groups over JCDC activities. For example, coordination with the Treasury Department includes detailed financial sector information that multiple interviewees found to be more relevant than JCDC engagement. This is not necessarily a failure, since sector-specific entities should be extensively coordinating; however, interviewees highlighted that information is not always shared between JCDC participants and sector-specific fora. Further streamlining information sharing, including outlining how different U.S. government entities coordinate private-public cybersecurity collaboration and how relevant information will be shared between those actors, would lead to more coherent and efficient collaboration between government and private actors within specific sectors.

Examples of JCDC Success

» In July 2022, JCDC coordinated a joint public-private sector effort to investigate and provide support to a cybersecurity incident involving the Albanian National Agency for Information Society (AKSHI). AKSHI shared key information with JCDC, allowing for further information sharing with industry partners resulting in the development of analysis products. JCDC also facilitated connections between the victim organization and U.S.-based entities that could provide AKSHI with direct assistance.[38]

» In December 2021, in response to the Log4Shell vulnerability in Apache Log4j software, JCDC shared indicators of compromise and threat intelligence among its members, fostering operational collaboration. Partners took immediate action to address the widespread threat affecting various consumer and enterprise services.[39]

View more examples of JCDC's successes.

38 "JCDC Success Stories | CISA," Cybersecurity and Infrastructure Security Agency, accessed December 1, 2023, https://www.cisa.gov/topics/partnerships-and-collaboration/joint-cyber-defense-collaborative/jcdc-success-stories.

39 "JCDC Success Stories | CISA," Cybersecurity and Infrastructure Security Agency.

The Ransomware Task Force

In late 2020, the Institute for Security and Technology (IST) convened the Ransomware Task Force (RTF). The RTF brings together over 60 members of software companies, government agencies at the local and national level, cybersecurity vendors, financial services companies, civil society, and academic institutions and representatives of national and local governments to address the threat of ransomware.[40] As stated in the RTF's foundational report, the members sought to "innovate new solutions, break down silos, and find effective new methods of countering the ransomware threat."[41] The RTF, as a multi stakeholder coalition, had the freedom to make recommendations that the government or private actors alone could not.

Public-Private Collaboration Mechanisms

The RTF has three formal means of collaboration with the private sector:

Leadership roles: Co-Chairs and Steering Committee

The RTF is organized around four goals, namely "Deter Ransomware Attacks," "Disrupt the Ransomware Business Model," "Help Organizations Prepare," and "Respond to Ransomware Attacks More Effectively." The RTF's foundational report, "Combating Ransomware: A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force" contains recommendations to advance each of these four goals. RTF leadership is composed of eight co-chairs who shepherded a number of large working groups and moved the report from idea formulation and recommendation drafting for each goal, to consensus and publication. Of the eight co-chairs, half were affiliated with civil society organizations while the other represented corporations relevant to combating ransomware. Six had previous experience working for the U.S. government, bringing to the effort an understanding of the limitations and opportunities that governments face when addressing ransomware and other cyber threats. These include challenges in information sharing and the difficulty of the

40 Unlike the other two case studies in this report, the RTF was not established through legislation. Rather, it is a civil society-led initiative.

41 "Ransomware Task Force (RTF) Combating the Ransomware Threat With a Cross-Sector Approach," Institute for Security and Technology, accessed February 8, 2024, https://securityandtechnology.org/ransomwaretaskforce/.

lawmaking and regulatory process. Most of the co-chairs also brought significant experience as conveners of stakeholders to make policy decisions or recommendations to their role. For example, Michael Daniel, the CEO of the Cyber Threat Alliance and an RTF co-chair, previously served as the Cybersecurity Coordinator for the U.S. National Security Council Staff, a role that required adjudicating disagreements between different U.S. government agencies.

Additionally, the RTF has a Steering Committee consisting of senior stakeholders and experts that provide top-level strategic advice, complementing the active role of the co-chairs in the coalition. The committee regularly meets with IST staff leading specific lines of effort, and, based on their senior positions in industry-leading companies and organizations, contribute valuable insights, guide decision-making processes, and enhance the overall impact of the RTF's effectiveness.

Ransomware Task Force Report

In April 2021, the RTF launched the Task Force's foundational report, containing 48 specific and actionable recommendations aimed at mitigating ransomware. When drafting the report, the co-chairs actively sought diverse perspectives to synthesize into a cohesive view to determine the most feasible next steps. The RTF also emphasized recognizing and accepting points of disagreement, and focusing on areas where progress would be possible. The RTF prioritized maintaining confidentiality, especially when involving government officials, adhering to strict standards throughout the process. The drafting process from inception to publication spanned four months, with dedicated working groups actively contributing for approximately two months to shape the specific recommendations presented in the final report. The RTF Co-Chairs, Steering Committee, and the staff at the Institute for Security and Technology (including the authors of this report) continue to work with the multistakeholder community to advance implementation of those recommendations, both in the United States and globally.

Ongoing Lines of Effort

The RTF actively engages in five key lines of effort, each dedicated to addressing distinct challenges within the ransomware ecosystem and driven by the recommendations in the original report. These efforts include the Cyber Insurance Roundtable Series, Payments Working Group, Blueprint for Ransomware Working Group, Victim Notification Working Group, and the International Engagement Working Group. These working groups go beyond mere assessment of the problem, leveraging insights from the RTF report to actively tackle specific issues.

For instance, the Payments Working Group, which comprises representatives from law enforcement, cryptocurrency analysis firms, technology providers, and security researchers, actively seeks strategies to disrupt the financial flows of ransomware actors and other cybercriminals. Through collaborative efforts, this group explores approaches to disrupt ransomware-driven financial transactions. Simultaneously, the International Cyber Engagement Working Group convenes monthly to exchange insights on various national/regional initiatives aimed at mitigating ransomware.

Why Does the Private Sector Participate in the RTF?

» **Focus on effective solutions:** Participants in the RTF were explicitly invited to engage with the group on the premise that the discussion would be oriented towards specific, actionable recommendations that could actually be implemented. The invitees who chose to engage did so because they saw the value of a cross-sector, practical approach to combating ransomware.

» **Access to a neutral ground:** The non-profit setting of the RTF offers a neutral ground, facilitating cooperation among private sector entities, government agencies, and other stakeholders. This neutrality is crucial, particularly when industry players may be hesitant to engage directly with the government, and may also be reluctant to engage directly with business rivals. As a non-profit convener, IST bridges the gap between policymakers and various subject matter expert communities, fostering open dialogue and trust.

» **Government advocacy and public goods issue:** The private sector actively participates in the RTF to advocate for more effective government intervention and coordination. Ransomware is a common threat, and the collaboration serves as a mechanism to address and coordinate actions, particularly in the absence of an established coordination mechanism.

Key Aspects That Drive the RTF's Success in Partnering

» **Open collaboration approach:** The success of the RTF's partnering efforts can be attributed to an open collaboration approach. The conveners did not arrive with a

pre-defined agenda, avoiding a prescriptive "we know what to do" approach. Instead, they openly acknowledged the need for collective expertise, showing up with a plan to seek input from participants with relevant experience/knowledge to help guide the initiative.

- **Emphasis on action and clarity of scope:** The RTF adopted a strategic and focused perspective in its policy recommendations. In its foundational 2021 report, recognizing the severity and specificity of the ransomware threat, the RTF provided 48 targeted recommendations. The scope of the report included a commitment to making concrete, actionable and reasonable recommendations that governments could implement in a short to medium timeframe.
- **Expertise in framing recommendations:** RTF leaders with prior government experience possessed the expertise to craft recommendations that facilitated government receptivity. By leveraging their understanding of government operations and policies, RTF leaders ensured that recommendations were relevant to governmental priorities.
- **Inclusive decision-making approach:** RTF leaders succeeded by recognizing the importance of proposing solutions grounded in multiple perspectives. They entered into the partnership aiming to ensure all voices were heard and taken into account in the Task Force's recommendations, cultivating a collaborative and inclusive effort.
- **Flexibility in partnership launch and operation:** Flexibility in both the initial setup and ongoing developments facilitated the success in establishing the RTF. To launch the RTF, the Task Force invited and convened a diverse cross-section of participants, encompassing technical expertise, policymaking acumen, and strong interpersonal skills.
- **Expanding participant network effectively:** The extensive networks of the RTF leaders facilitated the expansion of participants in the initiative. Willing to leverage their connections, these leaders proactively reached out to both private and public sector entities and individuals, fostering collaborations with those interested in contributing to the RTF. This inclusive approach aims to involve many private sector actors at the working level who are working day-to-day to combat threats at the technical level. Those individuals are often overlooked in high-level working groups but often possess valuable insights into what needs to be done and the obstacles faced.
- **Tracking recommendation progress**: Monitoring the progress of recommendations is a proactive measure that goes beyond merely advocating for change. The RTF continues to develop progress reports on its original recommendations. These evaluations provide valuable insights into the areas where progress has been achieved, and where additional policy changes across government and industry may be necessary.

» **Technology neutral:** The RTF focused on widely applicable principles, rather than addressing vulnerabilities or threats to specific systems or providing a specific technical solution. While RTF follow-up efforts have looked at how to apply widely-used approaches such as the CIS Controls, the initial report did not prescribe specific technological solutions.

Challenges to the RTF Partnership

» **Requires civil society volunteers:** The RTF faces a distinct challenge in its reliance on civil society volunteers who are already active in civil society work. While the U.S. culture of philanthropy has facilitated this approach, including through funding for the Institute for Security and Technology that enabled it to serve as the convening organization, not all countries have comparable access to organizations with philanthropic purposes and flexible funders. Varying cultural and structural contexts could make replicating the U.S.-based RTF, which relies on the contributions of engaged volunteers, challenging to replicate in other settings. This underscores the need for these types of collaborations to be adapted to different civil society landscapes, ensuring effective engagement with civil society representatives in regions with diverse approaches to community involvement.

» **Addressing U.S. centricity challenges:** The RTF has navigated challenges associated with the U.S.-centric nature of some of its recommendations (e.g., references to the U.S. Department of Treasury implementing sanctions), meaning that its recommendations may require adaptation to different national contexts. Despite the occasional default to U.S.-specific concerns, the RTF staff members seek to track progress on the original 48 recommendations worldwide, acknowledging advancements made beyond U.S. borders.

» **Challenges in promoting cyber hygiene practices:** One interviewee noted the difficulty faced by the RTF in effectively disseminating practical cyber hygiene best practices for small and medium enterprises (SMEs). Despite the RTF's efforts to develop proactive measures and policies to enhance entities' resilience against ransomware, the task of reaching out and ensuring widespread adoption, especially among SMEs, poses a significant challenge.

» **Translating varied inputs into actionable results:** In launching the RTF, consolidating diverse inputs from meetings and swiftly transforming them into actionable outcomes at breakneck speed was a challenge that the group overcame through substantial

individual commitment. The overall process took four months from inception to first publication.

» **Navigating diverse perspectives:** Managing various viewpoints poses challenges, and requires acknowledging that unanimous satisfaction may not be achievable. Despite this, the Task Force began with a shared commitment to productivity and consensus-building. It also sustained a remarkable degree of agreement with respect to the final product.

» **Strategic selection of pillars:** As the RTF's work is rooted in four foundational goals, the Task Force faced the challenge of careful selection. These goals would not only guide its original recommendations, but also shape the Task Force's ongoing implementation. Beyond initial selection, the Task Force actively determined the necessary phases for each goal, including specific timeframes for individual recommendations under each goal.

» **Managing expectations**: Navigating the uncertainty for next steps following the publication of the foundational report was a challenge cited by interviewees. The emphasis on disseminating the report, coupled with the coincidental release timing with the Colonial Pipeline ransomware attack, also brought higher expectations and a spotlight on immediate implementation.

Examples of RTF Success

» 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. An example of this is the U.S. government's creation of the Counter Ransomware Initiative (CRI) in November 2021, which aligns with RTF recommendation 1.1.2: "establish an international coalition to combat ransomware criminals."

» The Blueprint for Ransomware Defense, released in 2022, addresses RTF Report recommendation 3.1.1. by providing a recommendation of specific cyber hygiene safeguards based on the CIS controls. An analysis by the CIS Community Defense Model indicates that implementing these safeguards defends against over 70% of the attack techniques associated with ransomware.

View more examples of RTF successes.

Who is included in the multistakeholder model?

The "multistakeholder model" within the governance of the Internet and other technology-related policy, emphasizes the importance of inclusion of civil society organizations, profit-making companies, and relevant communities of experts, advocates, academics, and technologists in conversations about the Internet and security. While governments and the private sector often seek to collaborate, non-government non-profit entities can also bring a unique perspective and substantial expertise to these efforts.

Within different national contexts, the inclusion of non-government entities may take a range of forms. The academic community may include non-profit think tanks, academic institutions like universities and research centers, and representatives of the technical community, such as standards-setting bodies or independent cybersecurity researchers. Civil society organizations, like youth public service organizations or human rights advocacy organizations, may also offer expertise, such as in conducting public awareness campaigns useful for teaching effective cybersecurity practices. Intelligence sharing organizations or other cyber-focused nonprofits bring substantial capabilities to collaborative efforts. Additionally, non-profit and cooperative entities that operate critical infrastructure, such as hospitals, water plants, or electric power providers, are particularly relevant for counter-ransomware work, as these are often targets of ransomware incidents.

For a discussion of engaging stakeholders in cybersecurity policy approaches, refer to the Global Partners Digital publication, "Multistakeholder Approaches to National Cybersecurity Strategies." Additionally, refer to the United Nations Office of Drugs and Crime's report on "Internet Governance: Why the Multistakeholder Approach Works."

Global Best Practices

In synthesizing insights from our three case studies, we aim to distill global best practices and lessons learned in collaboration between government and the private sector in combating ransomware. These insights, drawn from our examination of Europol's European Cybercrime Centre (EC3), the Cybersecurity and Infrastructure Security Agency (CISA)'s Joint Cyber Defense Collaborative (JCDC) in the United States, and the Institute for Security and Technology's Ransomware Task Force (RTF), highlight critical and foundational characteristics that underpin the success of these initiatives. These best practices transcend specific contexts, forming a basis for effective PPPs in the global battle against ransomware.

Theme 1: Successful PPPs include a relevant and tailored range of stakeholders.

- **Actively seek participants that represent key stakeholders to address the problem that is being tackled by the partnership.**
- **Do not neglect civil society, the technical community outside of private industry, and the academic communities.**
    - Diversity of participants–in terms of experience, sector, and areas of expertise–can be valuable, because while a solution might work for one individual and their unique context, another group member could provide insights into its feasibility or potential challenges in a different sector or setting. This is critical for cyber risks that span sectors, such as ransomware.
- **Consider clearly delineating leadership roles, such as a specialized group or groups, to inform and guide the efforts of the PPP.** The designated entity or entities can serve as a focal point, facilitating strategic decision-making within the PPP.
- **Adapt to priorities and the social and cultural context in which the PPP is being convened.** This may include adapting to different contexts in terms of resources available, the capacity levels of participants, and seeking unique opportunities offered by the context in which the PPP is being convened. For example, a PPP in a country that hosts the headquarters of a major regional or global organization could consider offering that organization a distinct role in the PPP. A question to consider is:

    - In what ways can the PPP navigate and adapt to the unique economic considerations and resource availability of each participating country, locality, and/or entity?

- **Consider the number of participants.** Preserving trust and cohesion within the group is critical, and the size of the group plays a key role in this dynamic. Conveners of PPPs need to include all critical stakeholders, while ensuring that the group remains small enough to build trust between participants. Excessive numbers of contributors can dilute the collaborative environment, potentially leading to communication challenges and a diffusion of responsibility.
- **Prepare contributors actively.** Ensure that the selected participants receive briefings and are ready to contribute meaningfully to the initiative.
- **Consider a vetting process for potential PPP participants.** All three cases under investigation in this study either employed a review process for the initial participation of participants in the PPP or informally assessed participants' work before PPP leadership formally invited the entities to join the partnership.
- **Acknowledge the varied drivers and motivations of each participant.** Ensure that private actors understand that government counterparts—who operate under specific mandates and restrictions—follow established processes for a variety of reasons. This recognition ensures the credibility each participant brings to the collaborative effort, propelling the partnership forward and driving its success.
- **Regularly assess and, if necessary, update the composition of participating entities to align with the evolving landscape of ransomware and other cyber threat challenges.**

Theme 2: Successful PPPs catalyze effective information sharing.

- **PPP leaders—both private entities and government actors—should engage in robust exchange and feedback.** Share information bi-directionally, between the public sector to private sector, and between private sector entities.
    - Multiple interviewees commented that they particularly appreciated feedback from government actors about whether the information they shared was helpful, relevant, or timely.
    - Conversely, private sector participants indicated that they sometimes can go weeks, months or even without any response from government actors about information shared—not even a confirmation that the government appreciates the

information and would like to continue to receive it. For those actors, this lack of response is demoralizing and reduces the likelihood they will continue to share information or persist in the partnership.

- **Plan for a reasonable, reliable, and steady level of work when possible.** Information sharing has to be set up on a regular basis if it is going to be available for urgent cases. Having a regular cadence of meetings, non-meeting communication, and effective back and forth communication builds the "muscle memory" that will allow for surge processes when there are specific urgent threats.
- **Set expectations that all participants will contribute relevant information where they can, rather than free riding on the information shared by others.**
- **Set expectations about how information will be protected and shared within and outside the group.**
- **Know when to accommodate a partner's communication preferences.** For example, if a specific partner is known for consistently bringing accurate and beneficial information, but chooses to share one-on-one as opposed to in a group setting/chat forum, the PPP leadership should actively welcome that sharing and seek to use that information in an anonymized or non-specific way within the broader line of effort.
- **Strategically employ a blend of both formal and informal information sharing tactics, platforms, and agreements.** To make these work, PPP leaders need to:
  - Provide clear guidelines on data sharing, privacy, and use limitations. The guidelines should also lay out the legal context in which the sharing will occur; for example, participants should know whether sector-specific regulators participating in the partnership will be able to (or required to) share information with entities tasked with oversight duties (see spotlight on page 9).
  - Consider leveraging a platform that facilitates real-time, ongoing communication alongside asynchronous methods such as email.
  - Safeguard the confidential sharing of information as needed, including utilizing established information sharing designation methods like the Traffic Light Protocol (TLP, see spotlight on page 22) to communicate the sensitivity level of the shared information.
  - Acknowledge that while a degree of formality is necessary to maintain security and confidentiality, an overly rigid approach can become a barrier to effective

communication. Adaptability is key to navigating this delicate balance, ensuring crucial information reaches the right individuals and organizations promptly.

» **Organize training sessions, such as scenario-based exercises that simulate real-world ransomware incidents.** Such sessions allow participants to practice and refine their information sharing protocols collaboratively.

Information Sharing and Regulatory Oversight

One significant factor determining whether private companies are willing to share information with the government is the fear that sharing this information will open them up to legal liability and regulatory action by national cybersecurity authorities, law enforcement, and other government regulators. This fear may stem from potential misuse of shared information or the legal implications of collaboration, creating a barrier to open and transparent information exchange between private sector and government entities. Addressing these concerns early on in the formation of a partnership is therefore essential.

Concerns of this nature frequently arise when private entities consider sharing information about incidents they have experienced in their networks. In one interview, a former member of a national computer security incident response (CSIRT) team noted that the CSIRT had explicitly promised not to disclose information explicitly shared with the CSIRT with regulatory agencies. When governments set the terms of their information sharing agreements, they should consider whether this type of provision would be feasible in their national context. Above all, government actors must be clear about how information will be shared with other government agencies, and they must strictly adhere to their commitments in order to build trust and protect fragile and critical relationships with private entities.

Theme 3: Successful PPPs build trust through clear expectations and person-to-person collaboration.

» **Preserve confidentiality for enriched conversations**. Multiple interviewees emphasized that maintaining confidentiality creates a secure space where participants feel empowered to contribute candid and valuable insights. Actively adhering to rules like the Traffic Light Protocol or the Chatham House Rule during meetings not only safeguards the source of information, but also enriches the quality of conversations. This principle is particularly critical when conveners of PPPs invite government entities to engage in discussions, as it ensures they feel comfortable sharing their views.

» **Share results from information sharing.** Seeing concrete results from shared information actively contributes to building trust. Witnessing the practical benefits of their contributions, whether in the form of successful joint initiatives, improved counter

ransomware measures, or effective responses to threats, solidifies participants' sense of trust.

» **Incorporate face-to-face collaboration.** Trust is often built on relationships, and face-to-face interactions offer an opportunity to develop and strengthen these connections. One participant mentioned that informal discussions during meeting or conference breaks or networking events contribute to a more holistic understanding of each other's perspectives. Being physically present in meetings can also foster a sense of accountability. Participants are more likely to fulfill commitments and actively contribute when they have a personal connection with their counterparts.

» **Avoid unnecessary rotation of contributors.** Building a trust foundation in PPPs to combat ransomware necessitates stability and continuity among participants. As such, constant turnover of contributors can hamper the trust-building process. If it becomes necessary to switch out individuals who represent a particular entity within the PPP, strive to introduce the new team member(s), whenever possible. This step helps to ensure their integration into the PPP.

» **Actively collaborate and share resources.** One interviewee noted that no single institution operates in isolation against ransomware or cybercrime threats. This imperative emerges as the linchpin for making a tangible difference. Contributors need to see each other as reliable partners working together toward a common goal. Additionally, this collaborative approach is not just about short term action; it is about ensuring that the impact that individuals or organizations bring to the partnership is known, appreciated, and contributes meaningfully to the collective defense of digital infrastructure.

» **Make realistic commitments and follow through on them.** Establishing and preserving credibility, especially in collaboration with law enforcement agencies—whether as another public entity or as part of the private sector—hinges on making realistic and achievable commitments. One interviewee highlighted that law enforcement agencies are discerning in selecting private sector partners, underscoring the need for private entities to actively demonstrate genuine capabilities. In sum, this helps to manage expectations within the partnership.

Theme 4: Successful PPPs learn to navigate practical hurdles.

» **Acknowledge the limitations in bandwidth that affect all parties involved.** Different organizations may experience limitations based on their geographical location or size of

their staff. Recognizing these variations allows for flexibility in communication protocols and the development of adaptive strategies that accommodate the diverse needs of all stakeholders involved.

» **Recognize knowledge gaps.** In voluntary partnerships, such gaps–areas where participants may lack full visibility or access or capacity–naturally exist. PPP participants should keep this in mind, recognizing that questions they may have are likely shared by others. It becomes vital to proactively raise questions in order to bridge knowledge gaps and propel the partnership forward. Rather than perceiving knowledge gaps as obstacles, participants should be encouraged to view them as opportunities for collective learning and growth.

» **Prepare for resource inequalities.** Disparities in resources among public and private partners can hinder effective collaboration. Government agencies may have different budgetary constraints and technological capabilities compared to private sector organizations. Therefore, establishing strategic partnerships with external entities or organizations that can supplement the capabilities of the collaboration is vital.

» **Accept that partnership building is time-intensive.** Building robust PPPs to combat ransomware takes time, as participants engage in the intricate process of establishing trust, aligning objectives, and implementing effective communication channels among diverse stakeholders. Trying to short-change this process will weaken the partnership. Individuals involved in these partnerships often juggle multiple priorities, including their professional responsibilities and the need to demonstrate the strategic value of their time spent on contributing to collaborative efforts, which extends the time required to build the collaboration.

Steps to Setting Up Public Private Collaboration to Combat Ransomware

1. Define the goals of the collaboration.

Decide what specific element of the problem you want to tackle, such as tracking ransomware payments, identifying trends and the nature of the threat, prevention, and top-level information sharing. As much as possible, set goals for making progress against the selected problem, articulate timelines to achieve those goals, and then track the collaboration's progress. Identify and articulate minimum contributions for each participant (e.g., requirements to share specific types of data), and the ideal best-case scenario for your achievements.

Questions to address:

- What specific problem will this effort tackle?
- What is the outcome we are seeking to achieve?
- How will we define success?
- What does each participant need to contribute?
- How long do we expect this effort to take?

2. Identify the key relevant stakeholders and gauge their interest.

Which stakeholders should participate will depend on the purpose of the initiative; the number of stakeholders you invite to participate will also depend on the partnership's goals. Building trust is easier with a smaller group of stakeholders, but the group needs to have collaboration with key stakeholders relevant for the given goals. Particularly for government-led partnerships, the conveners should establish criteria for selecting group members and also criteria for engaging with specific entities outside the group when they are relevant to a

specific issue or incident. Such criteria do not have to be formalized, but conveners should be able to articulate them if asked.

Before formally inviting a partner to join the group, the group leaders and organizers should secure a commitment by both the entities at a corporate or senior level and from the individuals who would be contributing on a working level.

Questions to address:

- Who should join the effort? Why?
- How many stakeholders should be included?
- How can their participation be secured? Who should be asked first, who should confirm participation?

3. Establish the ground rules for the partnership.

This step involves establishing how the partnership or collaboration will operate. It covers a wide range of activity, such as meeting cadence, policy decision processes (e.g., consensus or voting), and review procedures for outputs such as reports (i.e., determining whether silence is equal to consent). One of the key elements includes setting expectations for the frequency and intensity of engagements, including at the working level and at the management level. Effective collaboration is not a "parachute in" scenario where government actors come to the group only when they have a need; rather, in effective partnerships, government representatives are regularly engaged with private sector participants to build a regular cadence of collaboration.

This also includes identifying the legal frameworks and standards under which information sharing will occur. Participants have to know whether other participants have specific restrictions or obligations regarding how they will handle information that is shared (e.g., law enforcement or intelligence information sharing obligations or restrictions).

This effort should also set expectations about the pace of engagement in the partnership and expectations about sharing, such as making information sharing a two way street. The rules should be clear about what kind of information the government can share and what private sector actors can do with it; similarly, it should be clear what will happen with information that the private sector shares within the partnership. Address concerns relating to sharing information between government entities, and any legal implications of "sunlight" or "freedom of information" laws. As with the second step, these ground rules do not necessarily have to be formalized in a written document and they can evolve as the partnership progresses.

Questions to address:

- How will the group make decisions?
- What procedures will the group use to review outputs, such as reports, press releases, or briefings?
- Will the partnership use the Traffic Light Protocol or another method of categorizing information to protect confidentiality and control sharing outside of the group?
- What methods will the partnership use to share information?
- What existing information sharing platforms will be used?
- Are formal agreements necessary?
- Are new information sharing agreements required?
- How much security is required for communications?
- Will information be shared between government departments, and which ones?
- What legal and liability issues do we need to address?

4. Start with trust-building practices.

Someone has to be willing to take the first step. Invite the strongest actors (e.g., larger, more capable companies, governments with intelligence assets, etc.) to share information first. Get to know the individuals who will be contributing, and seek to facilitate informal trust building exercises.

Questions to address:

- What can we do to kickstart trust building? How can we get to know one another at the organizational and individual level?
- How do we cultivate communication?
- What communication platforms will we use? How can we ensure they are accessible and secure at the same time?

5. Look for opportunities to achieve progress.

The partnership will probably not produce outcomes on a steady basis; progress will likely prove episodic. Therefore, participants should be ready to take opportunities to make progress when they occur. For example, there may be occasions when a particular actor is in the news, or when time sensitive information is shared. Use these opportunities to advance progress for the group, both in terms of achieving wins to address the specific threat, and

in terms of strengthening the mandate and institutional practices of the collaboration. Use successful outcomes and lessons learned to refine the framework of the PPP.

Questions to address:

- Do we have specific procedures for time sensitive information?
- How would we activate “surge capacity” protocols?

6. Continue to refine protocols, convening methods, and the overall structure/goals of the partnership as needed.

Recognizing that partnerships naturally progress through phases, conveners should regularly gather feedback from all participants. Soliciting insights and experiences ensures a responsive and adaptable framework. By fostering an environment that encourages continuous improvement, the partnership can effectively address emerging challenges and capitalize on opportunities, ultimately enhancing its overall effectiveness in combating the ever-evolving threat of ransomware.

Questions to address:

- How will participants provide feedback to the organizers?
- How will we measure success? Do those measurements need to change?
- When will we evaluate the effectiveness of this effort?
- How will we communicate to participants and to the public about our efforts?
- How do we decide on any shifting priorities?
- What milestones do we need to achieve for the effort to be effective?

INSTITUTE FOR SECURITY AND TECHNOLOGY
www.securityandtechnology.org

info@securityandtechnology.org