RANSOMWARE TASK FORCE

Combating Ransomware

A Comprehensive Framework for Action: *Key Recommendations from the Ransomware Task Force*

Prepared by the Institute for Security and Technology

IST Institute for SECURITY + TECHNOLOGY

Contents

A Note from RTF Co-Chairs 3-4
Executive Summary 5-6
Introduction 7-19
Ransomware as a National Security Threat 8
Understanding Ransomware 11
Ransom Payments 12
Cyber Insurance and Ransomware 13
The Role of Cryptocurrency 14
A Global Challenge 15
The Threat Actors 16
Existing Efforts to Mitigate Ransomware Attacks 18
A Comprehensive Framework for Action: 19-48
Key Recommendations from the Ransomware Task Force
Goal 1: Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy 21
Goal 2: Disrupt the ransomware business model and decrease criminal profits 28
Goal 3: Help organizations prepare for ransomware attacks 35
Goal 4: Respond to ransomware attacks more effectively 42
A Note on Prohibiting Ransom Payments 49-50
Conclusion 51
Summary of Recommendations 52-54
Acknowledgments 55-56
Appendices 57-72
Appendix A: Cyber Insurance 58-61
Appendix B: The Cryptocurrency Payment Process 62-67
Appendix C: Proposed Framework for a Public-Private Operational Ransomware Campaign 68-72
Glossary 73-76
Endnotes 77-81

Short cut: To go directly to each section in the PDF please click on the section title in the Contents.

This report is published under a 4.0 International Creative Commons License (see terms here).

A Note from the RTF Co-Chairs

We are honored to present this report from the Ransomware Task Force. This report details a comprehensive strategic framework for tackling the dramatically increasing and evolving threat of ransomware, a widespread form of cybercrime that in just a few years has become a serious national security threat and a public health and safety concern.

Ransomware is not just financial extortion; it is a crime that transcends business, government, academic, and geographic boundaries. It has disproportionately impacted the healthcare industry during the COVID pandemic, and has shut down schools, hospitals, police stations, city governments, and U.S. military facilities. It is also a crime that funnels both private funds and tax dollars toward global criminal organizations. The proceeds stolen from victims may be financing illicit activities ranging from human trafficking to the development and proliferation of weapons of mass destruction.

Tackling ransomware will not be easy; there is no silver bullet for solving this challenge. Most ransomware criminals are based in nation-states that are unwilling or unable to prosecute this cybercrime, and because ransoms are paid through cryptocurrency, they are difficult to trace. This global challenge demands an "all hands on deck" approach, with support from the highest levels of government.

Countless people around the world are already working tirelessly to blunt the onslaught of ransomware attacks. But no single entity alone has the requisite resources, skills, capabilities, or authorities to significantly constrain this global criminal enterprise.

For this reason, we convened the Ransomware Task Force — a team of more than 60 experts from software companies, cybersecurity vendors, government agencies, non-profits, and academic institutions — to develop a comprehensive framework for tackling the ransomware threat.

Our goal is not only to help the world better understand ransomware, but to proactively and relentlessly disrupt the ransomware business model through a series of coordinated actions, many of which can be immediately implemented by industry, government, and civil society. Acting upon a few of these recommendations will not likely shift the trajectory, but the Task Force is confident that implementing all of them in coordination, with speed and conviction, will make a significant difference.

While we have strived to be comprehensive, we acknowledge there will be areas we have not addressed, or on which we could not come to consensus. Prohibition of payments is the most prominent example; the Task Force agreed that paying ransoms is detrimental in a number of ways, but also recognized the challenges inherent in barring payments. Just as we have been grateful to stand on the shoulders of those that came before us, we hope our efforts and investigations will fuel the thinking and recommendations of those that come after us.

We urge all those with the ability to act to do so immediately. The ransomware threat continues to worsen by the day, and the consequences of waiting to respond could be disastrous. More than money is at stake; lives, critical infrastructure, public faith in the legitimacy of our institutions, the education system, and in many ways, our very way of life depends on taking action.

As a final note, we would like to offer our sincere thanks to the members of the Ransomware Task Force, who responded to our call and generously dedicated their time and energy into developing the recommendations included in this report.

The Working Group Co-Chairs of the Ransomware Task Force.

John Davis,
Palo Alto Networks

Megan Stifel,
Global Cyber Alliance

Michael Phillips,
Resilience

Kemba Walden,
Microsoft

Jen Ellis,
Rapid7

Chris Painter,
The Global Forum on Cyber Expertise Foundation Board

Michael Daniel,
Cyber Threat Alliance

Philip Reiner,
Institute for Security and Technology

Executive Summary

Ransomware attacks present an urgent national security risk around the world. This evolving form of cybercrime, through which criminals remotely compromise computer systems and demand a ransom in return for restoring and/or not exposing data, is economically destructive and leads to dangerous real-world consequences that far exceed the costs of the ransom payments alone.

In 2020, thousands of businesses, hospitals, school districts, city governments, and other institutions in the U.S. and around the world were paralyzed as their digital networks were held hostage by malicious actors seeking payouts. The immediate physical and business risks posed by ransomware are compounded by the broader societal impact of the billions of dollars steered into criminal enterprises, funds that may be used for the proliferation of weapons of mass destruction, human trafficking, and other virulent global criminal activity.

Despite the gravity of their crimes, the majority of ransomware criminals operate with near-impunity, based out of jurisdictions that are unable or unwilling to bring them to justice. This problem is exacerbated by financial systems that enable attackers to receive funds without being traced. Additionally, the barriers to entry into this lucrative criminal enterprise have become shockingly low. The "ransomware as a service" (RaaS) model, allows criminals without technical sophistication to conduct ransomware attacks. At the same time, technically knowledgeable criminals are conducting increasingly sophisticated attacks.

Significant effort has been made to understand and address the ransomware threat, yet attackers continue to succeed on a broad and troubling scale. To shift these dynamics, the international community needs a comprehensive approach that influences the behavior of actors on all sides of the ecosystem, including deterring and disrupting attackers, shoring up preparation and response of potential victims, and engaging regulators, law enforcement, and national security experts. We also need international cooperation and adoption of processes, standards, and expectations.

This report outlines a comprehensive framework of actions (48 in total) that government and industry leaders can pursue to significantly disrupt the ransomware business model and mitigate the impact of these attacks in the immediate and longer terms. These recommendations were collaboratively developed by the Ransomware Task Force (RTF) — a broad coalition of volunteer experts from industry, government, law enforcement, civil society, cybersecurity insurers, and international organizations — to provide a strategic framework for a systemic, global approach to mitigating the ransomware problem.

While we have identified some recommendations as priorities, we strongly recommend viewing the entire set of recommendations together, as they are designed to complement, and build on each other. The strategic framework is organized around four primary goals: to deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; to disrupt the business model and reduce criminal profits; to help organizations prepare for ransomware attacks; and to respond to ransomware attacks more effectively.

Priority recommendations

These priority recommendations are the most foundational and urgent; many of the other recommendations were developed to facilitate or strengthen these core actions:

1. Coordinated, international diplomatic and law enforcement efforts must proactively prioritize ransomware through a comprehensive, resourced strategy, including using a carrot-and-stick approach to direct nation-states away from providing safe havens to ransomware criminals.

2. The United States should lead by example and execute a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign, coordinated by the White House. In the U.S., this must include the establishment of 1) an Interagency Working Group led by the National Security Council in coordination with the nascent National Cyber Director; 2) an internal U.S. Government Joint Ransomware Task Force; and 3) a collaborative, private industry-led informal Ransomware Threat Focus Hub.

3. Governments should establish Cyber Response and Recovery Funds to support ransomware response and other cybersecurity activities; mandate that organizations report ransom payments; and require organizations to consider alternatives before making payments.

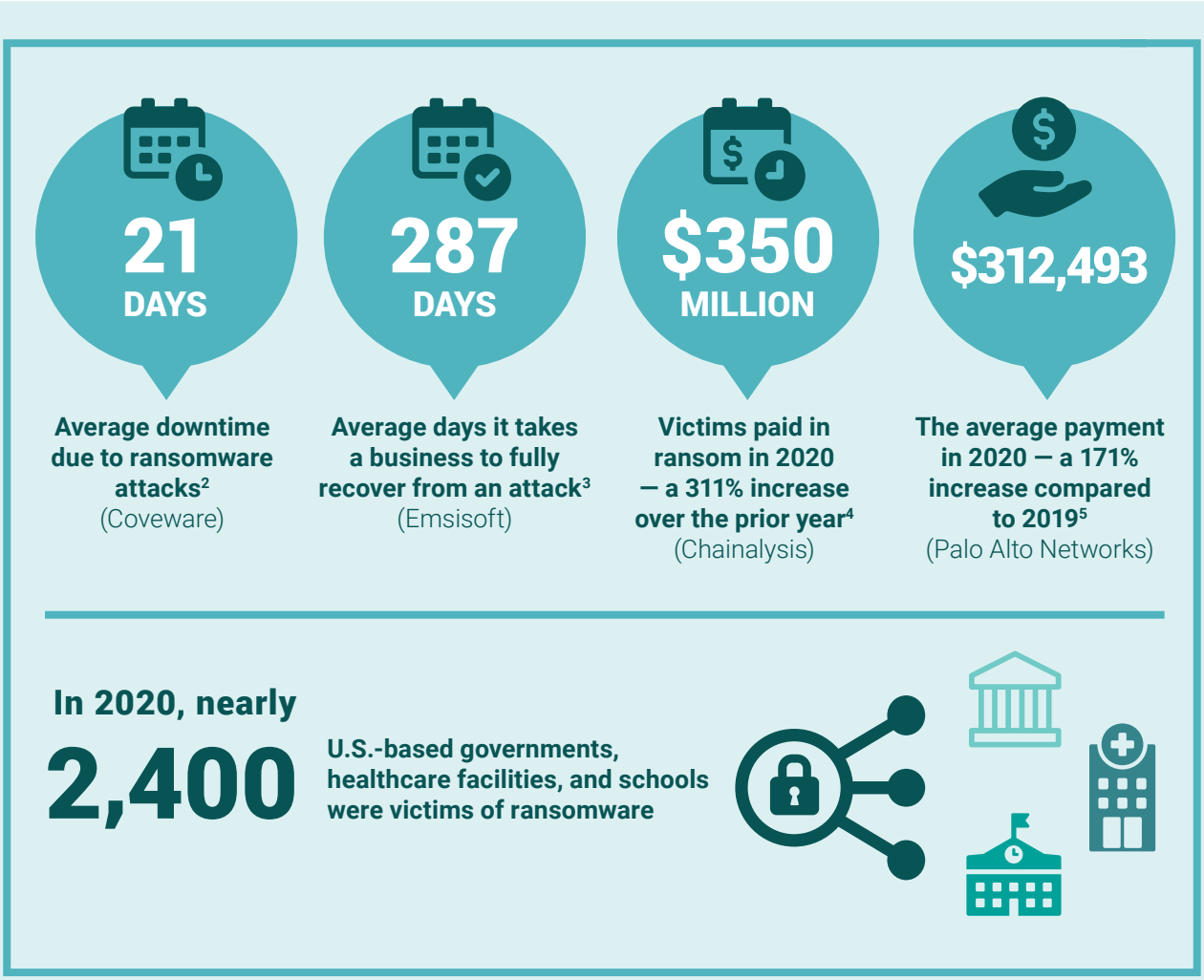
4. An internationally coordinated effort should develop a clear, accessible, and broadly adopted framework to help organizations prepare for, and respond to, ransomware attacks. In some under-resourced and more critical sectors, incentives (such as fine relief and funding) or regulation may be required to drive adoption.

5. The cryptocurrency sector that enables ransomware crime should be more closely regulated. Governments should require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws, including Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws.

The ransomware threat continues to worsen daily. The actions detailed in this report need to be enacted together as soon as possible, and must be coordinated at a national and international level in order to have the necessary impact. We understand the gravity of this challenge, but we believe that if this framework is implemented in full, the international community could see a decrease in the volume of these types of attacks in one year's time. Proposing this framework is merely the first step, and the real challenge is in implementation. With every recommended action we aimed to work through the practical implications, and in most cases we present immediately actionable recommendations. The Co-Chairs of the RTF welcome the opportunity to discuss these findings and recommendations further to help achieve these goals.

Introduction

Ransomware is a flourishing criminal industry that not only risks the personal and financial security of individuals, but also threatens national security and human life. Businesses, schools, governments, hospitals, and nearly every other type of institution are regularly targeted, disrupted, and held hostage. The problem has steadily grown worse in recent years, and in 2020, nearly 2,400 U.S.-based governments, healthcare facilities, and schools were victims of ransomware, according to the security firm Emsisoft.[1] Multiple organizations have issued reports on the costs of ransomware, and while their exact figures vary, all consistently show a steady increase in the number of attacks — and damaging economic impact.



Ransomware as a National Security Threat

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.

Threats to Critical Infrastructure:

Ransomware attacks have shut down the operations of critical national resources, including military facilities. In 2019, a ransomware attack shut down the operations of a U.S. Coast Guard facility for 30 hours,[6] and in February 2020, a ransomware attack on a natural-gas pipeline operator halted operations for two days.[7] Attacks on the energy grid, on a nuclear plant, waste treatment facilities, or on any number of critical assets could have devastating consequences, including human casualties.

Risks to Public Health:

Hospitals and other medical centers are a favorite target for ransomware criminals. In 2020, 560 healthcare facilities were hit by ransomware attacks in the U.S. alone.[8] These incidents not only cost the victims millions of dollars in recovery, but they also have led to delays in patient treatment, and possibly loss of life. In September 2020, a ransomware attack led to the failure of computer systems at Duesseldorf University Clinic, requiring critically ill patients to be relocated to other facilities, and in the United States, an attack caused delays in treatment for cancer patients at the University of Vermont Medical Care and other facilities.[9]

Societal Impact: *Targeting the Health Care Sector*

In October 2020, hackers compromised the computer networks of roughly a dozen medical centers across the United States. These attacks forced the cancelations of surgeries and disruptions in patient care; the University of Vermont Medical Center (UVM) was forced to furlough or reassign about 300 employees as the hospital's networks were taken offline in the midst of the COVID pandemic, and patients were turned away from scheduled cancer treatments and other medical procedures. The company's President and COO estimated the attack would cost roughly $64 million before systems were fully restored.

"It feels like we are all alone and no one understands how dire this is,"

– UVM Nurse to the *New York Times*.[10]

Extensive cyber vulnerabilities across the healthcare industry create potentially lucrative targets for malicious ransom-seeking actors, driving the significant increase in attacks against healthcare facilities. Government policy choices regarding ransomware should focus on this critical threat: statistical analysis reveals that ransomware-driven delays in care in these healthcare systems invariably contributes to a loss of life due to the inability of patients to receive timely care.[11] This illuminates the risk to human life posed by these attacks – and yet the attackers continue to undertake these assaults with near impunity.

Diversion of Vital Public Resources:

Ransomware attacks on municipal governments are common. Such attacks not only divert public resources into illicit economies, but the victims incur costs that far exceed the ransoms alone. For example, in 2018, the City of Atlanta paid $50,000 in Bitcoin as ransom, but the total cost of the recovery exceeded $2.6 million, as the city was forced to pay for digital forensics, increased staffing, crisis communications, and other costs.[12] A ransomware attack similarly debilitated the City of Baltimore, leading to a range of negative impacts.

Loss of Data/Privacy:

Ransomware criminals are increasingly expanding their attacks to include "double extortion," whereby they first demand ransom to de-encrypt an organization's data, then threaten to release the data on to the internet unless additional ransom is paid. At the start of 2020, only one major ransomware group exfiltrated data for a second extortion, but by the end of the year, at least 17 other groups used this tactic.[13] The potential exposure of their data and ensuing legal liability (particularly in countries with strict data security laws) may be a critical factor in leading some victims to pay the ransom.

Disruption of Schools and Colleges:

The education sector has become a top target: during 2020, nearly 1700 schools, colleges, and universities in the United States were impacted by ransomware.[14] According to a report by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and the Multi-State Information Sharing and Analysis Center (MS-ISAC), 57% of all reported ransomware attacks in August and September 2020 were targeted at K–12 schools.[15] These attacks not only disrupt the schools' operations, but often include threats to leak confidential student data on the internet.

Societal Impact: *Cities Under Siege*

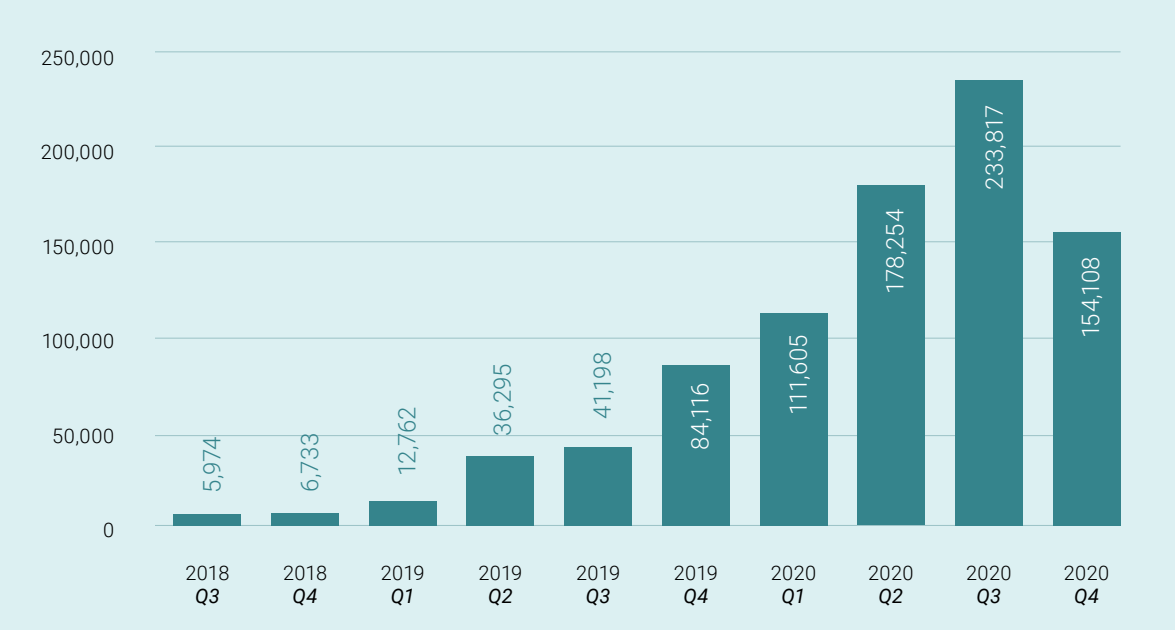
In May 2019, a ransomware attack on the City of Baltimore took critical services offline. The city refused to pay the ransom, but the recovery lasted several weeks and cost $18.2 million to restore systems back to their original state.[16] Beyond the financial burden on taxpayers and the shutdown of services, the city's inhabitants were no longer able to pay water bills, property taxes, or parking fines. Some residents who could not pay their bills saw their homes go into foreclosure. Databases tracking street drugs were knocked offline, people were unable to pay water bills and home sales were delayed.[17] The city's 911 dispatch system was knocked offline, and emergency calls made during that time were not recorded. The criminals threatened to publicly release data stolen during the attack to exert pressure on city officials to pay, in an early example of the "double extortion" tactic that has since become prevalent.[18]

Economic Impact:

Ransoms paid by private firms siphon millions of dollars toward criminal enterprise every year. The total amount paid by ransomware victims increased by 311% in 2020, reaching nearly $350 million worth of cryptocurrency.[19] However, the economic impacts go well beyond the costs of ransoms

alone. Reported ransomware payments do not cover the costs associated with service downtime and recovery. Total remediation costs are typically several times a ransom payment and are often large enough to cripple many small businesses. In addition, money that flows to the criminal networks creates second- and third-order economic effects, since those revenues go on to fund other types of crime.

FIGURE 1 Average ransom in USD



From The Coveware Quarterly Ransomware Report

Societal Impact: *K-12 Schools*

Ransomware attacks on schools have devastating impacts, including loss of instructional time and the leakage of sensitive data. In early 2021, a ransomware attack on the Buffalo Public School system prevented 5,000 students from returning to in-person learning Monday and shut down online learning for thousands more.[20]

Such attacks also add to budgetary challenges for already under-resourced districts: when Mississippi's Yazoo County School District paid $300,000 as a ransom to recover files encrypted during a ransomware attack, the cost equaled roughly 1.5% of the district's annual budget.[21]

The targeting of schools is not limited to the United States. In March 2021, a ransomware attack left 37,000 students in London and Essex without access to email or coursework. The attack targeted The Harris Federation, which runs 50 primary and secondary schools in the UK.[22] The perpetrators are suspected to have stolen personal data about the organization, including financial details, and posted it on the dark web.[23]

Understanding Ransomware

Ransomware is a sub-category of malware, a class of software designed to cause harm to a computer or computer network. CISA defines ransomware as "an ever-evolving form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption. Ransomware actors often target and threaten to sell or leak exfiltrated data or authentication information if the ransom is not paid."[24]

Ransomware proliferates in diverse ways, including through exploitation of vulnerabilities, as well as social engineering tactics, such as "phishing" emails that deceive employees within an organization to open attachments that launch the malware that then infects their networks. Once launched, the malware may connect to a command-and-control server to enable the criminals to move laterally across networks and encrypt and/or exfiltrate the organization's data. Ransomware victims are typically prompted with a screen informing them that their data has been encrypted, with instructions for how to restore their systems by sending payment via cryptocurrency. Not all attacks result in data encryption, but most do: a 2020 survey of 5000 IT managers found that 51% had been hit by ransomware in the last year, and the criminals succeeded in encrypting the data in 73% of these attacks, according to Sophos.[25]

Example of a ransomware lock screen

Ransomware victims are typically prompted with a screen informing them that their data has been encrypted, with instructions for how to restore their systems by sending payment via cryptocurrency.

Ransom Payments

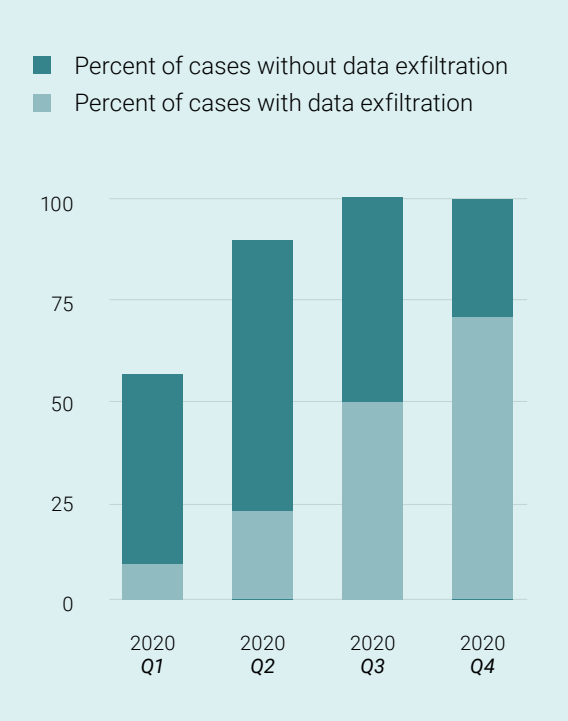
A number of factors can influence whether victims agree to pay the ransom demand, including whether they have cyber insurance, the quality of their data backups, and the estimated costs of the system outage. Legal considerations may also come into play: in the United States for example, firms that pay ransoms (and their facilitators) may find themselves in violation of regulations imposed by the Office of Foreign Assets Controls (OFAC).[26]

Surveys of global IT professionals have found that, of the organizations reporting a ransomware attack, 27% of victims chose to pay the ransom requested, with small variations at the regional level in terms of the average amounts paid $1.18 million in APAC, $1.06 million at EMEA, and $0.99 million in the United States).[27]

Victims may be more likely to pay if they are concerned their data will be made public. As a result, the theft and threat of public disclosure of sensitive data — a tactic known as "double extortion" or "data exfiltration" — has become an increasingly common tactic for ransomware attackers, as it intensifies the pressure on entities already struggling to regain operational capacity and protect sensitive data.

FIGURE 2

Percent of attacks involving data exfiltration



From The Coveware Quarterly Ransomware Report

Cyber Insurance and Ransomware

The cyber insurance industry sells policies to firms to cover losses in the event of a ransomware attack or other incident. Cyber insurance policies often include specific coverages for ransomware, including for business interruption losses, data restoration costs, incident response costs, and for a ransom payment, if one is made.

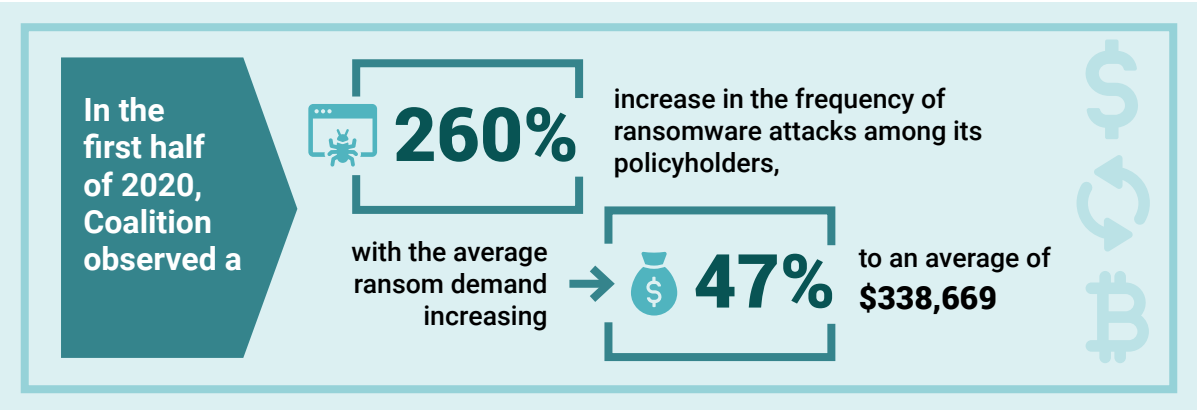
Ransomware attacks are the most common reported cyber insurance claim, according to Coalition, a cyber insurance firm. In the first half of 2020, Coalition observed a 260% increase in the frequency of ransomware attacks among its policyholders, with the average ransom demand increasing 47% to an average of $338,669.[28]

The role of cyber insurance in ransomware is complicated. Some argue that the "backstop" support of insurance encourages ransomware attackers, as victims may be more likely to pay if their costs are covered.[29] There is evidence that attackers may target companies specifically because they have insurance; in an interview, a ransomware criminal affiliated with the prominent syndicate REvil (also known as Sodinokibi) stated that targeting firms with cyber insurance was "one of the tastiest morsels."[30]

On the other hand, more mature insurance providers typically require that their clients adhere to strong baseline security practices, which can significantly reduce the disruption caused by a ransomware attack. They also connect victims to recovery experts and law enforcement, and can leverage a variety of market tools, such as co-insurance, to incentivize security standards and discourage organizations from paying ransoms.

The challenge is that not all cyber insurers are at the same level of sophistication, and some may even view a lack of security baseline requirements to be a unique selling proposition. Given the prevalence and cost of ransomware claims, it is rational to expect that the cyber insurance industry will eventually adopt security baseline requirements broadly as a standard expectation for insurability. When this becomes the status quo, insurers will play a more definitively positive role both in driving adoption of better cyber hygiene, and in providing an important safety net for victims of attacks. However, it will take time to achieve this maturity across the industry.

Acknowledging the ways in which cyber insurance may influence or shape organizational behavior and the ransomware "kill chain", the insurance-related recommendations in this report are designed to enhance the sector's role in supporting comprehensive public and private action against ransomware, while accelerating the cyber insurance market's maturity, solvency, and expertise. For a more detailed overview of cyber insurance, **see Appendix A**.



The Role of Cryptocurrency

The explosion of ransomware as a lucrative criminal enterprise has been closely tied to the rise of Bitcoin and other cryptocurrencies, which use distributed ledgers, such as blockchain, to track transactions. The use of cryptocurrency adds to the challenge of identifying ransomware criminals, as payments with these currencies are difficult to attribute to any individual. Often the money does not flow straight from ransomware victim to criminal; it travels through a multi-step process involving different financial entities, many of which are novel and are not yet part of standardized, regulated financial payments markets.

Ransomware criminals typically demand that victims send their ransom payments via Bitcoin, but after receiving the payment in a designated digital "wallet" (software that stores public and private keys), the criminals typically obfuscate these funds as quickly as possible to avoid detection and tracking. Their methods include "chainhopping," which involves exchanging funds in one cryptocurrency for another using any of a variety of cryptocurrency exchanges. The funds can be extremely difficult to trace after they have been exchanged, and to further shield themselves, ransomware actors may use money-mule service providers to set up accounts, or use accounts with false or stolen credentials.

Ransomware criminals can also obscure their transactions through cryptocurrency "mixing services," which muddy the public ledger by mixing in legitimate traffic with illicit ransomware funds. Some groups will also demand payments in currencies known as "privacy coins," such as Monero, that are designed for privacy and make payments untraceable.[31] However, privacy coins have not been adopted as widely as might be expected because they are not as liquid as Bitcoin and other cryptocurrencies, and due in part to regulation, this payment method may become increasingly impractical.

Cryptocurrencies add to the challenge of ransomware because they are considered to be "borderless." The cryptocurrency community is expressly focused on building a set of technologies designed to reduce compliance and financial process costs. After obfuscating the extorted funds, ransomware criminals may either withdraw the funds into hard cash, or because cryptocurrencies have become increasingly common (and their value has been steadily rising), they may keep their profits in cryptocurrency and use them to pay for other illicit activities.

While cryptocurrencies are difficult to trace, blockchain analysis can help interpret public blockchain ledgers and, with the proper tools, government agencies, cryptocurrency businesses, and financial institutions can understand which real-world entities transact with each other. Blockchain analytic companies are able to show that a given transaction took place between two different cryptocurrency exchanges, for example, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. With blockchain analysis tools and Know Your Customer (KYC) information, law enforcement can gain transparency into blockchain activity in ways that are not possible in traditional finance.

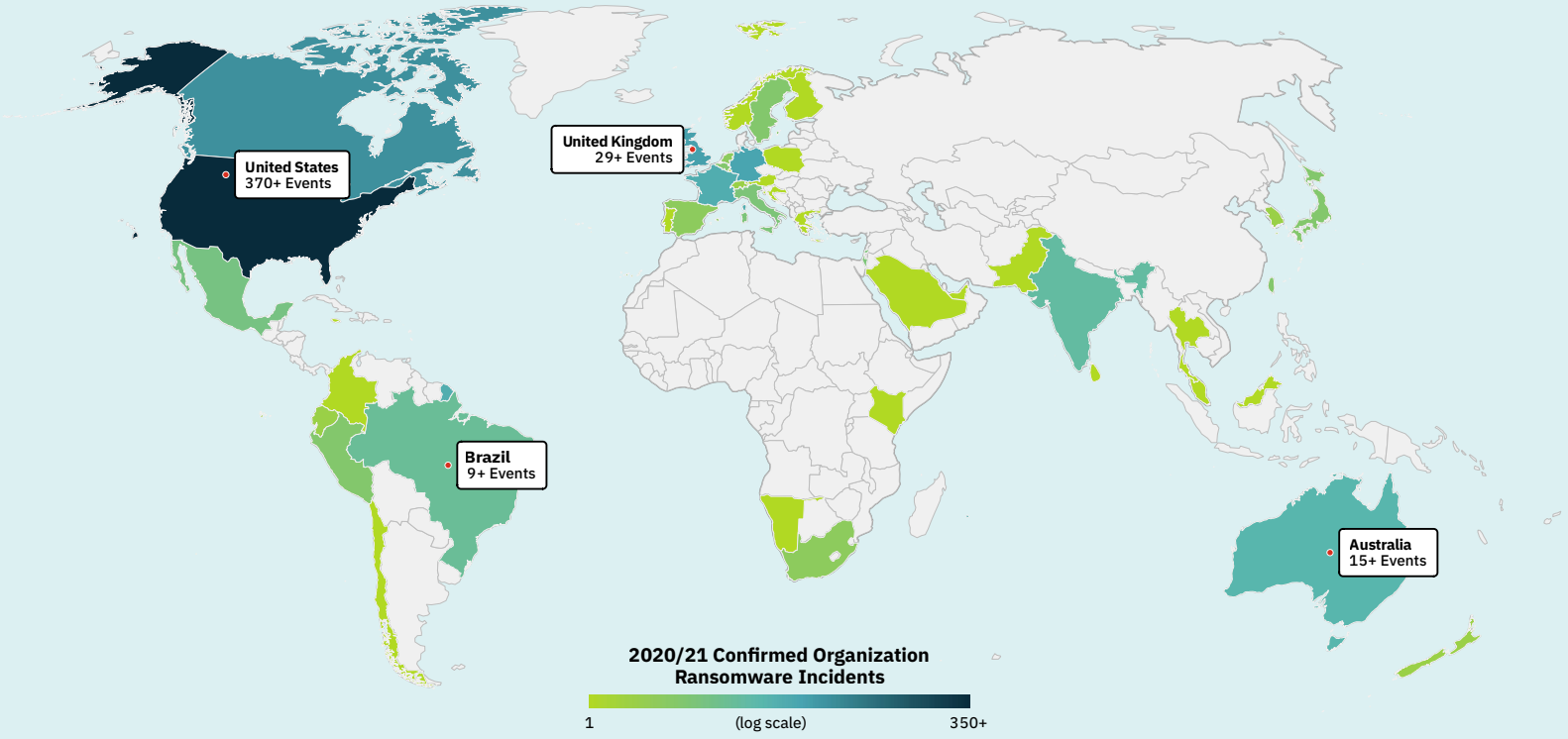
See Appendix B: The Cryptocurrency Payment Process, for a more detailed overview of how ransomware payments work, including where interventions could occur and how they could undermine the ransomware business model.

A Global Challenge

Ransomware is a global challenge, as institutions in all sectors around the world are being increasingly targeted. A single attack can also rapidly spread across borders, intentionally or otherwise: the 2017 WannaCry ransomware attack affected 150 countries.[32] A survey by security firm Sophos[33] found the nations with the highest percentage of organizations reporting ransomware attacks in 2020 were India, Brazil, Turkey, Belgium, Sweden, and the United States. However, ransomware attacks occur frequently in Russia, Saudi Arabia, China, and nearly every other nation.[34]

Reducing the ransomware threat will require global cooperation due to the highly decentralized nature of cryptocurrency, dispersed nature of the criminal networks involved, the internet's basic infrastructure, and the differing legal and regulatory regimes around the world. Ransomware criminals are able to game the system by moving their operations to where legislation and cybercrime enforcement are the most lenient. International institutions have begun to tackle this challenge: in October 2020, for example, finance ministers from the Group of Seven (G7) called upon nations to implement Financial Action Task Force standards to reduce ransomware and other cybercrime.[35] However, more must be done to improve global cooperation, reduce safe havens, align international standards, and ramp up enforcement.

FIGURE 3 2020/21 Confirmed Organization Ransomware Incidents



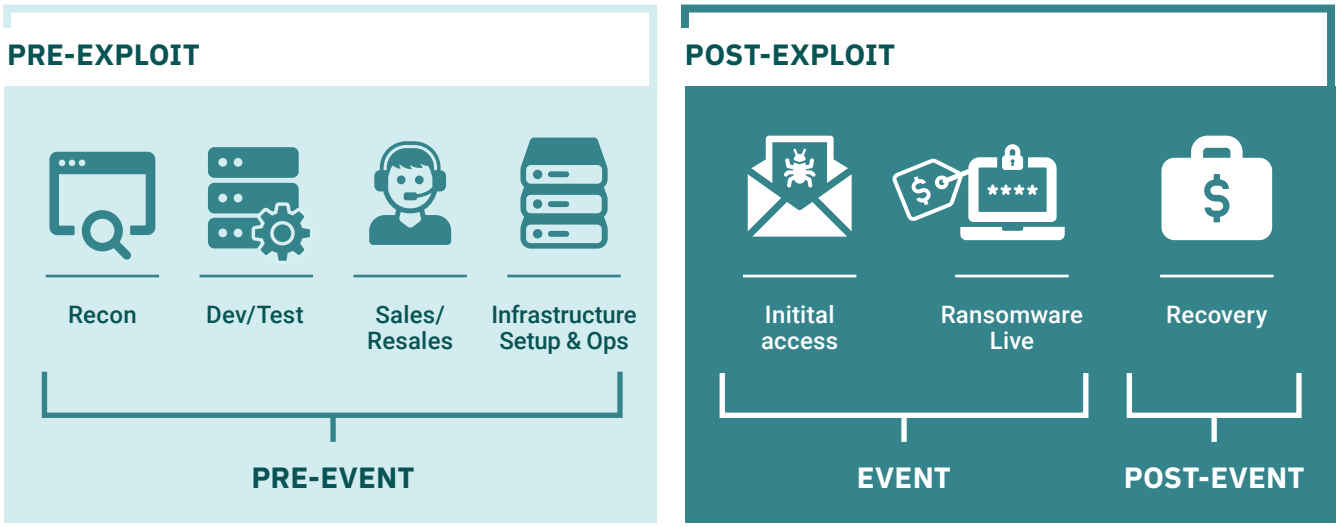
Sources: Palo Alto Unit 42; Scitum; Cloudian; Black Fog; Recorded Future Incidents include victim organizations with data published on leak sites or with publicly disclosed ransoms.

The Threat Actors

The profitability of ransomware has attracted a diverse set of malicious actors, who have built a thriving and evolving criminal ecosystem. While different ransomware attacks may seem similar, they are often executed by a diverse array of attackers with highly variable motivations. Some are organized into ransomware "gangs," which, like other organized crime units, operate in one cohesive team while developing and executing attacks.

Recent years have seen the rise of the "ransomware as a service" (RaaS) business model. Some national governments have used ransomware to advance their strategic interests, including evading sanctions. This diversity of threats increases the complexity of attributing and countering ransomware attacks and highlights the need for broad pressure along the entire ransomware kill chain.

FIGURE 4 Ransomware "Kill Chain"



Source: World Economic Forum's Partnership against Cybercrime in collaboration with Accenture

Ransomware-as-a-Service

Carrying out a ransomware attack does not require technical sophistication. "Ransomware as a service" (RaaS) is a business model that provides ransomware capabilities to would-be criminals who do not have the skills or resources to develop their own malware. In 2020, two-thirds of the ransomware attacks analyzed by cybersecurity firm Group-IB were perpetrated by cyber criminals using a RaaS model.[36] This "as a service" model follows similar evolutions in the mainstream software and infrastructure industries, which have seen success from "software as a service" and "infrastructure as a service" business models.

In the RaaS model, there are at least two parties who establish a business relationship: the *developer* and the *affiliate*. The developer writes the malicious program that encrypts and potentially steals the victim's data. The developer then licenses this malware to the affiliate for a fixed fee or a share of successful ransom payments. The affiliate executes the attack and collects the ransom, potentially also including additional business arrangements, like purchasing exploits or using cryptocurrency brokers and washers.

In this model, even a non-technical affiliate can successfully execute ransomware attacks by purchasing the necessary exploits and malware. RaaS can be contrasted with more traditional ransomware gangs, in which a cohesive team both builds the malware and executes the attack. The Sobinokibi, Phos, Dharma, and GlobeImposter ransomware variants are all known to operate under the RaaS model.[37]

The Nation-State Nexus

Of particular interest to the Task Force was the relationship between ransomware and national governments. Many ransomware criminals operate with impunity, as their countries' governments are unwilling or unable to prosecute this form of crime. In other cases, the organizations executing ransomware attacks may be state-sponsored, and may in fact be helping nations evade economic sanctions.[38] For example, in an April 2021 announcement of new sanctions against Russia, the U.S. Department of Treasury made a direct connection between Russia's Federal Security Service (FSB) and ransomware hackers, noting that "to bolster its malicious cyber operations, the FSB cultivates and co-opts criminal hackers, including the previously designated Evil Corp, enabling them to engage in disruptive ransomware attacks and phishing campaigns."[39]

Proceeds from ransomware may help finance terrorism, human trafficking, or the proliferation of weapons of mass destruction.[40] For these reasons, direct affiliation between ransomware attacks and governments is intentionally shrouded in secrecy, making attribution and accountability challenging. Countering state-sponsored attackers will require broad application of "carrot and stick" methods and international cooperation.

Societal Impact: *NotPetya*

The 2017 NotPetya attack highlighted how this form of cybercrime can have far-reaching consequences. The estimated financial losses exceeded $10 billion, but the true scale of the damage was far greater. Though the attack was not strictly ransomware as it was not motivated by profit, it did leverage ransomware code, cause the same type of disruptive impact, and present a screen demanding a ransom.

The attack started in Ukraine, where computer systems at two major airports, bus stations, railways, the postal service, and media companies were taken hostage. It infected ATM machines and payment systems, and for the first time after 31 years, the radiation monitors at Chernobyl shut down, forcing workers in hazmat suits to manually monitor radiation levels.[41]

The destructive virus was designed to spread, and soon shut down factories in locations as far away as Tasmania. NotPetya affected Merck's production of critical vaccines, and the company had to dip into emergency stockpiles to meet demand. Doctors in Virginia and Pennsylvania were locked out of patient records and prescription systems.

Two years after the attack, railway and shipping systems in Ukraine still were not working at full capacity. Packages that had been lost due to ransomware were still not found, and senior citizens continued to miss pension payments as their records had been lost.

NotPetya was a stark example of how ransomware attacks can affect the very functioning of a society, and erode the trust that citizens hold in public institutions.

Existing Efforts to Mitigate Ransomware Attacks

Ransomware is not a new problem. As attacks have increased in prevalence and impact, significant effort has gone into understanding and addressing the array of associated issues. This includes the development of technical tools, critical research on attacker groups and trends, best practice guides for preparation, established threat intel sharing programs, and attack nullification efforts.

The security field has well-known, pre-existing resources for cyber hygiene,[42] staff training,[43] and securing resources.[44] Cybersecurity firms can provide network monitoring, anomaly detection, and containment. Incident response teams have been established across government,[45] industry, and nonprofits, and at a systemic level, federal funding, information sharing, and public-private partnerships have been proposed to improve cyber response across organizations.[46]

Yet adoption of preparedness best practices remains limited, and ransomware attackers continue to find sectors and elements of society that are woefully underprepared for this style of attack. The sheer volume of content published on the topic of ransomware is part of the challenge; with so much information and noise surrounding this threat, time- and resource-constrained organizations and individuals struggle to identify the most relevant and accurate sources of useful information. In addition, many guides are reportedly either too simple, too complicated and overwhelming, or not specific to ransomware. Operational security and IT staff represented in the Task Force reported that it is a struggle to find guidance that is truly actionable and feels relevant to their needs.

Significant effort remains to address the increasing risks posed by ransomware attacks. The sheer volume of attacks hitting such a broad range of sectors leaves even private sector security companies often lacking the capacity to respond to the number of requests for assistance. In response, federal governments have taken steps to coordinate information sharing and raise awareness around the risks posed by ransomware: for example, in January 2021, CISA unveiled the Reduce the Risk of Ransomware Campaign to encourage public- and private-sector organizations to implement best practices, tools, and resources that can help them mitigate ransomware risk.[47] The U.S. The Dutch National Police, Europol, McAfee, and Kaspersky Lab founded an initiative called "No More Ransom", which provides decryption keys, information on ransomware, and preventative advice, and has done so for years.[48] The UK's National Cyber Security Centre also provides useful information and guidelines on how to mitigate ransomware.[49] Coordinated global law enforcement actions have led to isolated successes; in January 2021, for example, a coordinated effort led to the disruption of the EMOTET botnet, a major component of ransomware criminals' infrastructure.[50]

Despite these efforts, ransomware attacks have continued to grow almost unabated, and the criminals behind them continue to operate with near impunity. What began as a relatively minor nuisance to people and business is now causing losses in the billions of dollars, and attackers have continued to target critical public facilities like schools and hospitals. Solutions have been deployed in an uncoordinated, disjointed manner, with different sectors working on siloed solutions. The ransomware threat cannot be stopped via piecemeal solutions; it needs the dedicated, coordinated attention of experts, from policymakers to security engineers to industry leaders.

A Comprehensive Framework for Action:

Key Recommendations from the Ransomware Task Force

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. In response, in early 2021, the Institute for Security and Technology (IST) convened the Ransomware Task Force (RTF), an interdisciplinary group of leaders, for a three-month sprint with the goal of producing a comprehensive framework of actionable solutions and recommendations to help public- and private-sector leaders reduce the threats posed by ransomware in the near and long term.

This strategic framework aims to help policymakers and industry leaders take system-level action — through potential legislation, funding new programs, or launching new industry-level collaborations — that will help the international community build resistance, disrupt the ransomware business model, and develop resilience to the ransomware threat.

The framework is organized around four goals: ***deter*** ransomware attacks through a nationally and internationally coordinated, comprehensive strategy; ***disrupt*** the ransomware business model and reduce criminal profits; help organizations ***prepare*** for ransomware attacks; and ***respond*** to ransomware attacks more effectively.

These goals are interlocking and mutually reinforcing. For example, actions to disrupt the ransomware payments system will decrease the profitability of ransomware, thereby helping to deter other actors from engaging in this crime. Conversely, without taking the recommended steps to deter ransomware attackers, disruption will be harder to achieve. In a similar vein, many actions taken to better prepare organizations for ransomware attacks, such as informing them about the risks, will also improve their ability to respond, while understanding more about how organizations are responding to ransomware attacks will help improve organizations' collective preparedness. Thus, this framework should be considered as a whole, not merely a laundry list of potential disparate actions.

Recommendations at a glance:

1. *Deter Ransomware Attacks*

2. *Disrupt the ransomware business model*

3. *Help organizations prepare*

4. *Respond to ransomware attacks more effectively*

A Note on the U.S. Focus and International Application

Ransomware, like our digital world, knows no bounds. All of these recommendations seek to leverage the power of multi-stakeholder collaboration, nationally and globally, to combat a crime that transcends borders and attacks indiscriminately. Many recommendations, like enforcing compliance on cryptocurrency entities to drive ransomware actors out of business, will be unsuccessful without international collaboration. A single country's laws or capabilities will be insufficient to tackle this global threat.

While the Ransomware Task Force involved participants from around the world, the majority of members were based in the United States and were primarily familiar with the U.S. legal and policy landscape. As a result, and to help ensure our recommendations are specific and actionable, the findings and recommendations detailed in this report have a decidedly U.S.-focused lens. However, we believe many of the recommendations can and should also be translated to other jurisdictions.

The effort to combat ransomware will only be successful if carried out through a coordinated, international effort. The following recommendations carry universal themes, like improving ransomware preparedness in organizations. We encourage agencies and organizations in other nations — including cybersecurity, law enforcement, government and industry leaders — to adapt these recommendations to their own contexts, and work across borders to coordinate and tackle what is truly a global challenge.

Goal #1

Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy

The number of actors capable of conducting ransomware attacks is large and growing, and to curb the growth of this threat in the long-term, steps must be taken to systemically discourage ransomware attacks. This deterrence must be multilayered and rely on all instruments of national power. We propose a coordinated, effectively messaged, relentlessly executed deterrence campaign directed from the senior-most levels of the U.S. Government in real-time collaboration with international partners. The actions recommended here are to be directly supplemented by the disruption activities recommended in Goal #2.

Objective 1.1:
Signal that ransomware is an international diplomatic and enforcement priority

International governments must cooperate more purposefully and publicly to send an effective signal to ransomware criminals that this form of cybercrime is a diplomatic and law enforcement priority. A clear declarative policy will serve as a foundation to other international and national-level efforts.

Action 1.1.1: Issue declarative policy through coordinated international diplomatic statements that ransomware is an enforcement priority.

Using existing high-level forums (such as the G7, G7 Finance Ministers, G20, Interpol, Europol, and others[51]), senior-level officials and ministers from major nations should agree to one or more joint declarations condemning ransomware as a national security concern and/or a threat to critical infrastructure, and commit to pursue ransomware actors. There are several international[52] precedents[53] for this declarative policy. This declaration should outline the steps signatories will mutually agree to take, and include an agreement for each nation to create a domestic action plan.

Timing: *Begin immediately to lay the groundwork; declarations would be issued when the groups meet.*
Lead: *State Department, National Security Council (NSC), Treasury, Department of Homeland Security (DHS), and Department of Justice, in coordination with international partners.*

Action 1.1.2: Establish an international coalition to combat ransomware criminals.

A standing international coalition composed of representatives from key nations is necessary as a conduit for sharing information and other resources related to the ransomware threat. Such a coalition should include representatives from law enforcement using successful models like Europol's Joint Cybercrime Action Taskforce,[54] but also including the intelligence community, and private industry. It should carry out key shared

tasks, such as building a legal case against criminal actors, pursuing targets/groups through pooling resources and tools, and amplifying takedowns when they happen. This effort would directly coincide with those detailed in 1.1.1 and 1.1.3, but also throughout the actions recommended under Goal #2.

Timing: *3-6 months.* **Lead:** *White House, in coordination with international partners.*

Action 1.1.3: Create a global network of ransomware investigation hubs.

The U.S. Government should lead the development of a network of ransomware investigative hubs across the globe, including by leveraging cyber assistant legal attachés (ALATs) and International Computer Hacking and Intellectual Property (ICHIP) lawyers. The groups within this "team of teams" should be nimble and have access to specialists in each of the kill chain areas of the ransomware criminal organizations. The hubs should ensure their investigative priorities and resources are aligned and coordinated. They should foster a culture of information sharing, be located in diverse geopolitical regions to enable swift sharing of intelligence, and contribute directly to the coalition recommended above in Action 1.1.2, but also to the actions recommended below in Objective 1.2 and many of the actions under Goal #2.

Timing: *9-12 months.* **Lead:** *State Department, Department of Justice, and international equivalents.*

Action 1.1.4: Convey the international priority of collective action on ransomware via sustained communications by national leaders.

Any international effort will need to include coordinated public communications by national leaders to keep the spotlight on combating ransomware as a priority and ensure the success of the broader effort. These communications can take the form of speeches, op-eds, news articles, videos, and other media that draw attention to ransomware as a problem, promote prevention, and highlight enforcement successes.

Timing: *Begin immediately to lay the groundwork; declarations must be issued on an ongoing basis.*
Lead: *White House, in coordination with international partners.*

Objective 1.2:
Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House

Ransomware is an urgent threat that demands a "whole-of-government" strategic response. Within the U.S. Government, establishing structures for cross-agency coordination will be vital for tackling the ransomware challenge, and will reduce the lag time in government response. Leading new joint efforts with industry will also be crucial: no single actor is fully capable of disrupting this threat by themselves, so we must come together to assess the threat and coordinate activities across authorities and capabilities. Although this recommendation is U.S.-focused, a similar approach should be adopted by other national governments. Additionally, since ransomware is a cross-border issue, it will be vital for governments to reach out to, and work with, international partners both on a policy and operational level.

Action 1.2.1: Establish an Interagency Working Group for ransomware.

To ensure this challenge receives sufficient investment of time and resources from the highest levels of the U.S. federal government, the White House should establish an Interagency Working Group (IWG) dedicated to understanding and addressing the ransomware threat at a systemic level, and on an ongoing basis. Doing so will signal to ransomware actors and international partners that this issue rises above other pressing cybersecurity priorities. Ideally led through the National Security Council (NSC) in coordination with the new National Cyber Director (NCD), the Ransomware IWG will serve as a high-level strategic forum for coordinating expertise, shaping policy, sharing information, and directing action for all stakeholders.

The Ransomware IWG will also help ensure that intragovernmental conflicts can be escalated efficiently through the White House policy-coordination and national security decision-making process. The IWG should provide policy direction and leadership for all U.S. Government actions related to ransomware, which will improve accountability and help ensure that agencies work together on signaling and deterrence. In addition, the NSC/NCD, State Department, DHS, DOJ, Treasury, and other relevant members of the IWG should engage international allies and partners to build a like-minded coalition against ransomware and ensure policy coordination, as called for in Action 1.1.2.

Timing: *Immediate.* **Lead:** *White House and international equivalents.*

Action 1.2.2: Establish an operationally focused U.S. government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub.

The Interagency Working Group (IWG) described in Action 1.2.1 should direct and oversee the creation of an internal U.S. government Joint Ransomware Task Force (JRTF), whose objective is to coordinate an ongoing, nationwide campaign against ransomware, and identify and pursue opportunities for international cooperation. The JRTF's primary function is to identify targets for disruption and takedown, and clearly designate roles and responsibilities for each. The U.S. government needs this formal interagency structure to avoid uncoordinated activity and to break down the stovepipe structure. The JRTF must be empowered to leverage all tools of national power and should prioritize ransomware threats to critical infrastructure. The JRTF should increase the pace and efficacy of intelligence-driven ransomware infrastructure takedowns, disruptions of ransomware operations, and arrest and prosecution of the people that enable them. A detailed breakdown of a potential structure, roles, and responsibilities for the JRTF are provided in **Appendix C**.

The JRTF should collaborate closely with relevant private-sector organizations that can help defend against and disrupt ransomware operations, such as security vendors, platform providers, telecommunications providers, information sharing organizations, cybersecurity non-profits, and other capable entities. These private-sector activities and groupings can continue to operate on an informal and *ad hoc* basis through the establishment of a Ransomware Threat Focus Hub (RTFH), which can serve as a central, organizing node for informal networks and collaboration as part of a collaborative, sustained public-private anti-ransomware campaign. The structure, roles, and responsibilities of the RTFH are also provided in **Appendix C**.

Timing: *Immediate.* **Lead:** *White House, via the direction of the IWG, in coordination with private industry, and international equivalents.*

Action 1.2.3: Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign.

The JRTF should use all tools of national power to sustain an intelligence-driven anti-ransomware campaign that includes target identification, threat hunting, action planning, execution, and communications. The roles and responsibilities covered within the JRTF should include, but not be limited to: law enforcement action, diplomatic efforts, economic tools, technical cyber operations, and intelligence operations as appropriate. The campaign and capabilities utilized should be tailored to target specific vulnerabilities in ransomware groups and their operations as identified in the intelligence assessments recommended in Actions 1.2.5 and 1.2.6. Coordination of operations, and intelligence sharing that supports those operations, should be streamlined with exceptions to policy as needed to be most effective in targeting groups on the designated list. This should include sharing and operational coordination with U.S. government entities, private industry (e.g. cybersecurity companies, service providers, and trust groups), and a coalition of international partners.

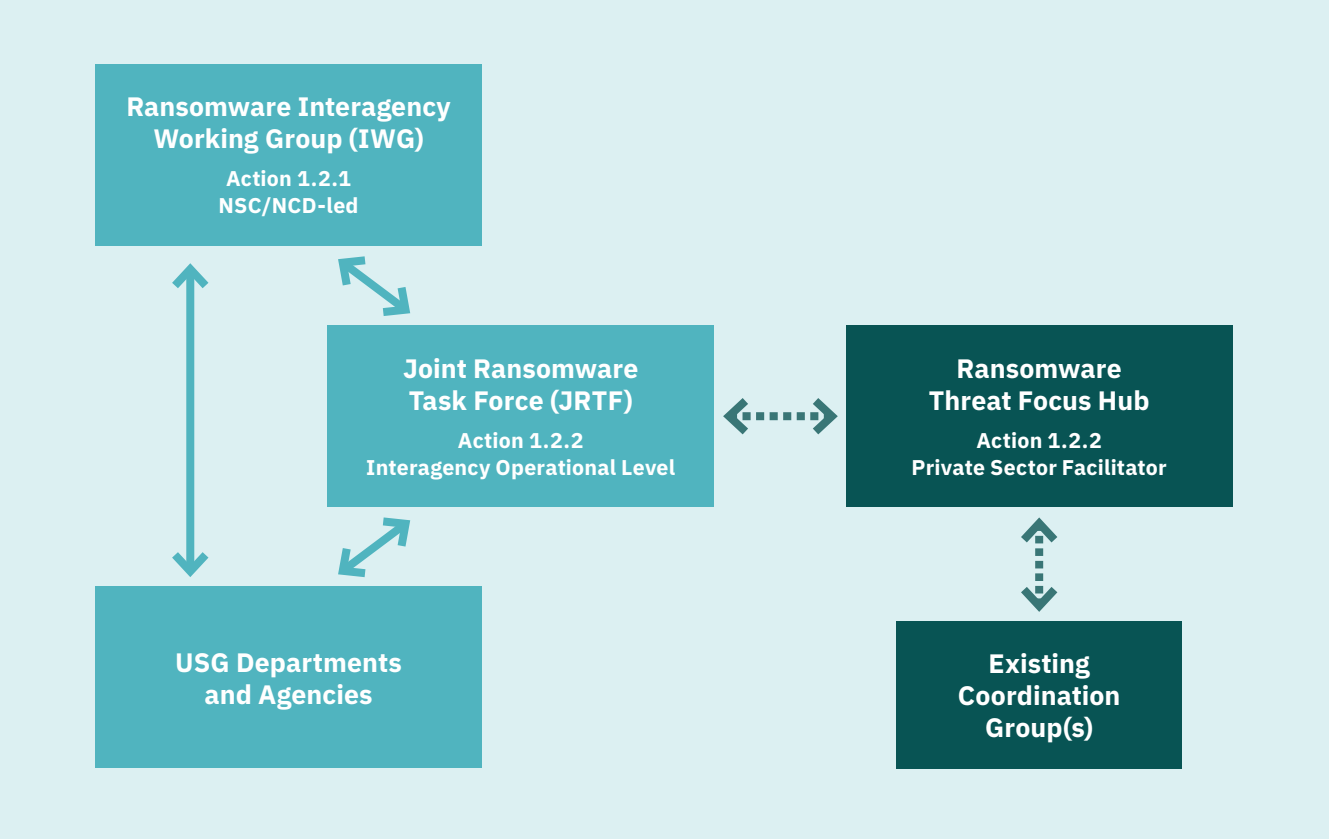
The JRTF should enhance operational coordination with their international counterparts to conduct more, and more effective, international investigations and take-downs. This would be directly facilitated through the investigative hubs recommended in Action 1.1.3. The JRTF should, to the greatest extent possible, operate at the unclassified level, which is essential to enable flexibility, quick reaction times, and the incorporation of essential partners who are not JRTF members. To make this possible, the U.S. government should follow the lead of its counterparts in the United Kingdom's National Cyber Security Center and dramatically increase the volume of TS/SCI information made available at the unclassified level, with a singular focus on the ransomware threat.

The JRTF can ensure agreements are in place with designated private-sector partners to allow for field level coordination, and must coordinate early and frequently with all relevant elements of U.S. departments and agencies, for instance, the NCIJTF and select U.S. Attorney Offices.

Via the private-industry Ransomware Threat Focus Hub (RTFH), as detailed in **Appendix C**, non-government participants in these campaigns could include infrastructure providers, platform/OS providers, registrars, endpoint security companies, threat intelligence firms, content delivery networks (CDNs), network operators, non-profits, and industry nodes. Engagement, planning, and execution should not be limited to regularly scheduled meetings; rather, the structure should allow for continuous, responsive, and ad hoc coordination and execution based on constantly changing events.

Timing: *3-6 months.* **Lead:** *White House, via the direction of the IWG in Action 1.2.1, in coordination with private industry, and international equivalents.*

FIGURE 5 Proposed Framework for a Public-Private Operational Ransomware Campaign



Action 1.2.4: Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public.

The Department of Justice (DOJ) recently formed an internal task force to tackle ransomware and the Acting Deputy Attorney General issued guidance making ransomware an investigatory priority. The Task Force supports this focus on ransomware and recommends that senior officials, such as the Attorney General, the Director of the FBI, and/or the Director of the United States Secret Service, sustain this focus at United States Attorney's Offices (USAOs), FBI field offices, and Secret Service Task Forces to more aggressively pursue cases against ransomware actors. Consistent with this guidance, USAOs should prioritize ransomware prosecutions and seek harsher penalties for attacks on critical infrastructure or for attacks that endanger public health and safety.

Legislation should also be considered to make ransomware and other Computer Fraud and Abuse Act offenses subject to RICO, given the organized crime aspects of these offenses. Additionally, to raise the level of priority and clearly communicate that new status, officials should also pursue asset forfeiture against ransomware actors to the maximum extent allowed by law and signal their intention to use this tool. This recommendation is expanded upon further in Actions 2.1.5 and 2.3.3.

Timing: *9-12 months.* **Lead:** *U.S. Department of Justice and Congress, and international equivalents.*

Action 1.2.5: Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat.

The United States must raise the Intelligence Community (IC) collection priority against ransomware actors so that all necessary resources, capabilities, and authorities can be brought to bear to answer the intelligence needs to fulfill the tasks of the IWG and the JRTF. These must include (but are not limited to): signals intelligence (SIGINT) (including computer network operations, or CNO), human intelligence (HUMINT), and imagery intelligence (IMINT). This elevated prioritization must be accompanied by a reduction in the roadblocks that impede greater bidirectional sharing of information between the IC, international IC partners, and private industry, in order to fulfill the intelligence needs of the IWG and the JRTF's campaigns.

To establish the baseline for target development, the NSC should task an Intelligence Community Assessment (ICA) focused solely on ransomware actors and the criminal-state nexus. The goal of this ICA should be to accurately capture: the nature of the ransomware threat to national security; identification of actors and groups who pose the most significant threat (including attribution to individuals involved whenever possible); locations from where they operate; and the infrastructure, tactics, and techniques they commonly use. The ICA should also detail vulnerabilities that may exist within each actor group; any relationships between the actors and their governments that could negatively impact law enforcement's ability to counter the threat; and any intelligence gaps that would need to be filled to more completely understand this threat.

Based on the findings in the ICA and any other relevant intelligence, the IC should clearly designate ransomware actors as a national security threat at the level appropriate to the findings, and raise the priority of actively countering the threat. The designation and priority level should ensure that all tools of national and international power are brought to bear to counter this threat in an aggressive, effective, but proportional, coordinated campaign, as is detailed in 1.2.3.

Timing: *3 months.* **Lead:** *White House to task DNI, coordinate with Five Eyes Partners and international equivalents.*

Action 1.2.6: Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns.

International partners should work together to develop an international Intelligence Community Assessment (ICA) on ransomware actors with the same goals described in Action 1.2.5 in order to create a more complete picture of the global security threat posed by ransomware actors, and to serve as the baseline for coordinated international efforts. An international ICA will help raise the global intelligence collection priority against ransomware actors so that all necessary resources can be brought to bear to answer the intelligence needs required to fulfill national and international collaborative efforts.

Timing: *3 months.* **Lead:** *White House to task DNI, coordinate with Five Eyes Partners and international equivalents.*

Objective 1.3:
Substantially reduce safe havens where ransomware actors currently operate with impunity

Many pernicious ransomware actors are given free reign by the nations where they reside and cannot be easily reached by international law enforcement agencies, either because a host country is actively protecting them, lacks the resources and capabilities to stop them, or does not prioritize the issue. Together with international partners, the U.S. should use a "carrot and stick" approach to motivate these nations to use all tools of national power — including critical law enforcement action — against the criminals operating within their borders or within friendly or neighboring countries.

Action 1.3.1: Exert pressure on nations that are complicit or refuse to take action.

Nations should exert pressure on other nations that refuse to take action against ransomware criminals. These strategies could include economic and trade sanctions; constrain "safe haven" country activity in international financial markets; using evidence of complicity to "name and shame" them in public forums to disrupt their freedom of activity; withholding military or foreign assistance aid; or denying visas to citizens who seek to travel to the United States or other nations. Actions undertaken by the JRTF and the RTFH to disrupt the ransomware business model should proactively be utilized to contribute to the intended deterrent effect of this sustained pressure campaign.

Timing: *3 months, ongoing.* **Lead:** *U.S. Department of Justice and U.S. Department of State.*

Action 1.3.2: Incentivize cooperation and proactive action in resource-constrained countries.

Some nations that serve as home bases for ransomware actors may not understand the gravity of this crime, or they may lack sufficient resources to prosecute ransomware criminals. The United States and other nations should provide training and capacity-building to support these nations' efforts, and provide direct law enforcement support, for example through joint law enforcement operations. Providing incentives to private-sector partners in those nations may also increase these nations' willingness to cooperate. Establishing ransomware as a priority in bilateral agreements could further bring these nations to the table.

Timing: *30 days and ongoing.* **Lead:** *U.S. Department of Justice and Department of State, and international equivalents.*

Goal #2

Disrupt the ransomware business model and decrease criminal profits

Ransomware is overwhelmingly a financially motivated crime, and as long as the profits outweigh the risks, attacks will continue. To effectively disrupt this threat, government and industry stakeholders must work collaboratively across borders to reduce the profitability of this criminal enterprise and increase the risk of ransomware execution. Governments can take diverse actions to:

1. *Disrupt payment systems to make ransomware attacks less profitable;*
2. *Disrupt the infrastructure used to facilitate attacks; and*
3. *Disrupt ransomware actors themselves, through criminal prosecution and other tactics.*

This must all be done while minimizing harm to the victims of ransomware and not interfering with their ability to recover their systems.

The flow of money from a victim to a ransomware actor using cryptocurrency is complex. See Appendix B for a detailed guide on this process, and how entities like cryptocurrency exchanges fit within this ecosystem.

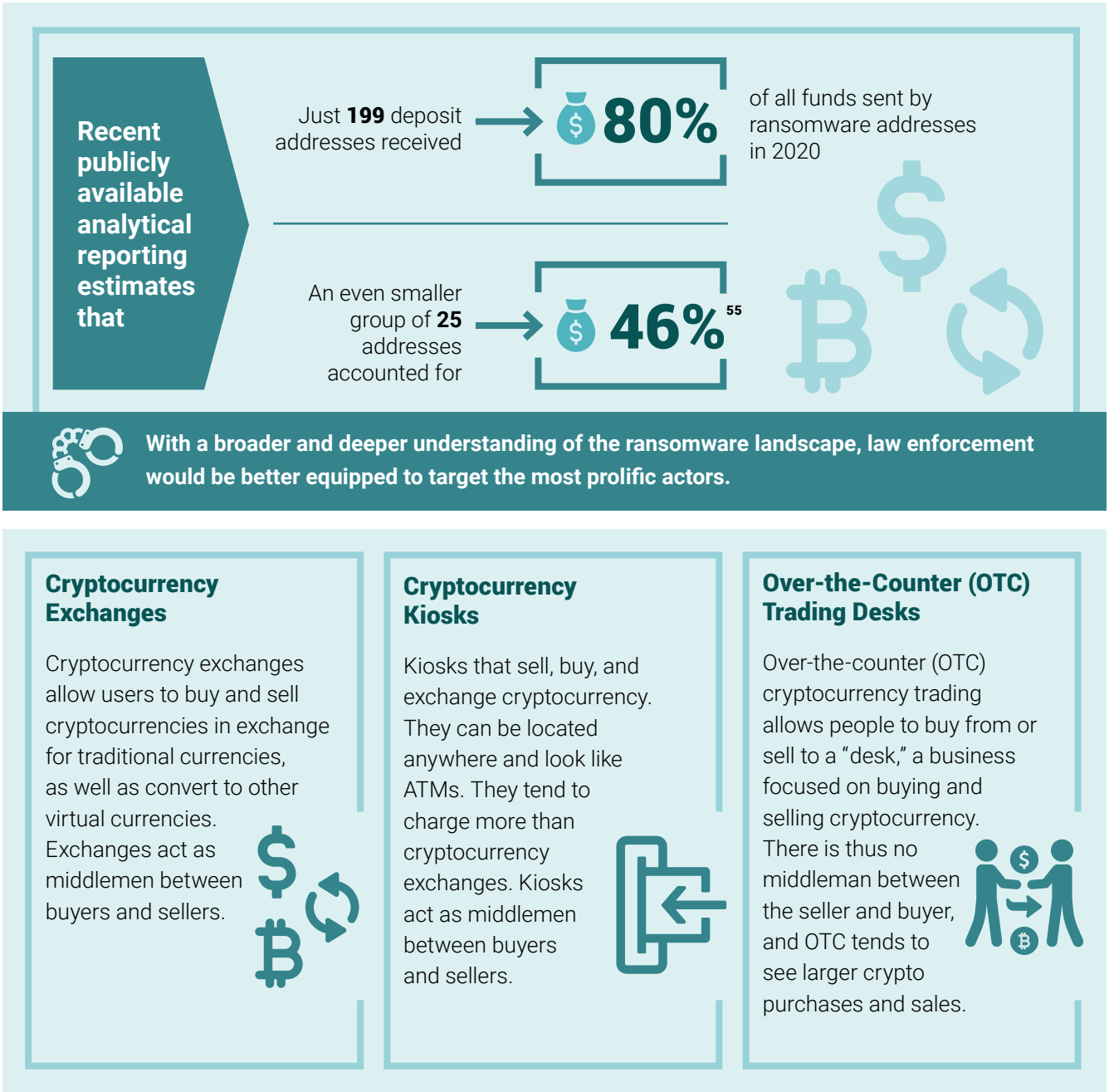
Objective 2.1:
Disrupt the system that facilitates the payment of ransoms.

Ransomware attacks are profitable because ransom payments are made through the use of diverse cryptocurrencies, where payments are difficult to trace and can easily be laundered. The challenge for governments is to find new ways to get inside the ransomware payments process. It will be important to set measurable goals to assess progress toward this objective.

Action 2.1.1: Develop new levers for voluntary sharing of cryptocurrency payment indicators.

In addition to the mandatory disclosure of a ransomware payment recommendation in Action 4.2.4, lawmakers should create incentives to share timely and actionable cryptocurrency payment indicators to enable law enforcement to prioritize leads and seize ransom payments when possible. This information may include wallet addresses, transaction hashes, and ransom notes. In exchange for this information, victims should be able to report anonymously, unless a victim is otherwise required to disclose the attack under privacy laws. Congress should broaden the Cybersecurity Information Sharing Act of 2015 to cover this type of information sharing, explicitly preserving attorney-client privilege and implementing parameters that limit how this information could later be used by regulators or as part of civil litigation, to encourage participation.

Timing: *6 to 12 months.* **Lead:** *Congress, CISA, and other international equivalents.*



Action 2.1.2: Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws.

Lawmakers need to pursue and enforce consistent licensing and registration requirements for cryptocurrency exchanges, crypto kiosks, and OTC trading desks where criminals "cash out" their cryptocurrency from ransomware payments. These entities are not consistently compliant with or subject to Know Your Customer (KYC), Anti-Money Laundering (AML), and Combatting Financing of Terrorism (CFT) laws, and those that are subject to those laws do not consistently report suspicious transactions to law enforcement or other institutions.[56] These laws must designate clear enforcement bodies to penalize non-compliant exchanges, kiosks, and OTC desks.

Traditional financial institutions that fund these entities should also impose stricter rules. They should pursue SEC enforcement of cryptocurrency businesses that fail to register as broker-dealers, transfer agents, clearing agencies, and money service businesses (MSBs), with particular focus on mixing services that obfuscate criminal transactions with legal traffic.

Timing: *12 months.* **Lead:** *Treasury Department, Securities and Exchange Commission, and other international equivalents.*

Action 2.1.3: Incentivize voluntary information sharing between cryptocurrency entities and law enforcement.

Regulators should incentivize cryptocurrency exchanges, crypto kiosks, over-the-counter trading desks, and financial institutions to increase their reporting of suspicious transactions to federal law enforcement, to facilitate joint disruptive actions. In the U.S., these entities would use Section 314(b)[57] reports and suspicious activity reports (SARs) to report suspicious transactions to the Financial Crimes Enforcement Network (FinCEN) of the U.S. Treasury Department. In addition, the Department of Treasury should streamline its processes for sharing SARs with exchanges, blacklisting wallets, and sharing with relevant federal and non-federal entities that may take other timely disruptive action.

Timing: *12 months.* **Lead:** *U.S. Treasury Department (FinCEN) and international equivalents.*

Action 2.1.4: Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes.

Law enforcement action on the basis of ransomware reporting must be swift as criminals strive to quickly move funds beyond their reach. In the U.S., law enforcement can provide a cryptocurrency exchange with a letter requesting that ransomware funds be frozen at the exchange as proceeds of crime to be seized by the government. If done in time and with cooperation from the exchange, this can make the identified funds unavailable to the ransomware actors. This letter must be followed up with a seizure order from an attorney within the Department of Justice, a process that, at the moment, is scattered across the United States, assigned to different investigations, and assigned to attorneys with varying experience drafting these orders.

Key units within the Department of Justice — including the Computer Crime and Intellectual Property Section (CCIPS), Computer Hacking and Intellectual Property Network (CHIPS), National Security Cyber Specialists (NCSC), the National Security Division (NSD), and the Money Laundering and Asset Recovery Section (MLARS) — should identify attorneys who are knowledgeable in civil and criminal seizures related to cryptocurrency, and engage them to serve as a focal point for seizure orders across ransomware investigations. This should be part of the campaign tasked to the JRTF described in Action 1.2.2 or to the recently formed DOJ ransomware-focused task force. This would dramatically streamline the current process, ensure seizure orders are pursued expeditiously, and increase the number of seizure orders served, thereby making it more difficult for ransomware adversaries to convert virtual currency to fiat.

Timing: *6 to 12 months.* **Lead:** *U.S. Department of Justice and international equivalents.*

Action 2.1.5: Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation.

For individual ransomware victims, the economics of pursuing civil remedies against liable actors may not make sense, given the case may require extensive factual investigation and innovative legal efforts. To solve this problem, insurers and reinsurers should measure and assert their aggregated ransomware losses and establish a common "war chest" subrogation fund to evaluate and pursue strategies aimed at subrogation recoveries, including restitution, recovery, or civil asset seizures, on behalf of victims and in conjunction with law enforcement efforts.

Many insurers currently maintain individual subrogation units, but these do not typically act within the context of ransomware. This is because insurers may not be familiar with the novel legal and investigative expertise needed to pursue ransomware actors; they may believe the chances of recovery are unclear, and the cases may span multiple international jurisdictions where insurers may not typically pursue subrogation. This common "war chest" subrogation fund may sit within a consortium (as described in Action 2.1.7) established by insurers and reinsurers to properly resource and scale novel efforts to pursue civil recoveries against liable actors, kickstarting efforts in civil courts to obtain justice, while pooling the costs associated with any one case, alleviating concerns about uncertain results.

Timing: *6 to 12 months.*
Lead: *Domestic and international insurance and reinsurance firms.*

What is subrogation?

Subrogation refers to an insurer's assumption of an insured victim's rights of recovery after a loss is covered and paid by the insurer. Subrogation empowers an insurer to pursue the rights of the insured to recover the amount of a loss from the parties who are legally liable for it. Subrogation thus serves to make both victim and insurer "whole" in the event of a civil recovery. For more information, **see Appendix A: Cyber Insurance**.

For Further Investigation: The Tax Enforcement Opportunity

The IRS and Europol have engaged in efforts to identify taxpayers who have failed to disclose income from cryptocurrency, including developing "tax evasion signatures" within cryptocurrency transactions. In 2021, the IRS's Office of Fraud Enforcement announced "Operation Hidden Treasure," convening trained IRS criminal agents and blockchain analysis firms to identify cryptocurrency-related tax fraud.[58] National and international tax authorities and interested policymakers should further investigate opportunities to leverage tax enforcement efforts like these in the fight against ransomware.

Action 2.1.6: Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs.

In 2012, the U.S. Securities and Exchange Commission (SEC) launched a whistleblower reward program that has already yielded several billion dollars in penalties that the U.S. would not have otherwise obtained. A public whistleblower campaign in this vein should be targeted toward geographic regions around the world, and provide awards for information leading to the identification of individuals involved with developing ransomware, money laundering of fiat, coding, ransom negotiations, and other roles. In addition to financial awards, such a program could include non-monetary rewards, such as a path to citizenship. Any reward program should be designed in a way to protect the anonymity of the reporter of the criminal activity.

Timing: *6 to 12 months.* **Lead:** *The Securities and Exchange Commission and international equivalents.*

Action 2.1.7: Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management.

Insurers and reinsurers should voluntarily establish an industry consortium to aggregate and share anonymized, pertinent data to support threat-actor disruption, including both payment information (such as wallet addresses, ransom demands, negotiation outcomes, and transaction hashes) and attack information.

Data sharing at the consortium should also accelerate the maturation of best practices and sustainability of the cyber insurance market, as this data enables further risk modeling and underwriting analysis. This consortium should improve risk management and resolution strategies so that ransomware is less frequent, less destructive, and less profitable for the threat actors. It should also enable insurers and reinsurers to establish certainty with law enforcement and regulators such as OFAC as to the legality of any payment and as with respect to sanctions. Finally, the consortium may serve as the home of any common subrogation "war chest" fund for collaboration, as described in Action 2.1.5. This consortium should also work directly with the JRTF and RTFH as described in actions 1.2.2 and 1.2.3.

Timing: *6-12 months (to establish consortium and initial subrogation effort).*
Lead: *Domestic and international insurance and reinsurance firms.*

Objective 2.2:
Target the infrastructure used by ransomware criminals

Ransomware actors rely on infrastructure to carry out their attacks, including servers and networks that serve as "command and control" for their attacks. Law enforcement agencies have opportunities to disrupt ransomware criminals by targeting this infrastructure.

Action 2.2.1: Leverage the global network of ransomware investigation hubs.

The global network of ransomware investigative hubs recommended in Action 1.1.3 (and utilized by the coalition recommended in 1.1.2 and the JRTF recommended in Action 1.2.2), including leveraging cyber assistant legal attachés (ALATs) and ICHIP prosecutors, should have access to specialists that are empowered to focus efforts

on infrastructure aimed at the "left of boom" elements of the criminal business model. This includes, among other areas, credential theft or other unauthorized access; malware distribution, including the use of malicious domains and criminal and abusive command and controls; criminal surveillance; and theft of intellectual property.

Timing: *6-12 months.* **Lead:** *U.S. Federal Government and international equivalents.*

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

Currently, private-industry companies — including but not limited to hosting companies, internet service providers, and telecommunications companies — are actively working with law enforcement and other industry partners to disrupt infrastructure associated with ransomware actors. This infrastructure may include malicious servers used to facilitate or conduct attacks against victims. If a service provider is tipped to malicious infrastructure, it should be able to take action against the infrastructure without fear of legal liability. For example, if a hosting company is made aware that a customer is conducting attacks from one of the hosting company's servers, they can typically shut down the customer's service due to a violation of the company's terms of service. In a less clear scenario, if a telecommunications company is provided a signature that identifies malicious network traffic and they block the traffic from transiting their network, thereby disrupting the malicious activity, the company may have some legal liability.

Congress should ensure private industry can actively block or limit traffic when acting in good faith without fear of legal liability. Specifically, Congress should modernize the Computer Fraud and Abuse Act (CFAA) and other cybersecurity laws to take into account activities that cybersecurity companies, security researchers, service providers, and other responsible parties are currently doing "at risk" in gray areas in order to protect their customers.

To be clear, this is not advocating for "hacking back," rather it is focused on decriminalizing practical security activities necessary to counter modern cybersecurity threats, including against criminal infrastructure like botnets used in ransomware.

Timing: *12 to 24 months.* **Lead:** *U.S. Congress and international equivalents.*

Objective 2.3:
Disrupt the threat actors, including ransomware developers, criminal affiliates, and ransomware variants

Action 2.3.1: Increase government sharing of ransomware intelligence.

The government should increase the sharing of intelligence about ransomware actors with the private and nonprofit sectors, including key data points that specifically lead back to the threat actors. Such information could include threat actor personas, tradecraft, and attribution (including roles and responsibilities); behavioral tactics and techniques; and related technical information (i.e., indicators of compromise). Making such intelligence more broadly available would enable the private sector to protect itself more effectively; better

coordinate with government entities, such as the JRTF and RTFH in Action 1.2.2; and support governments in disrupting ransomware activity.

Timing: *6 months and ongoing.* **Lead:** *Department of Homeland Security and international equivalents.*

Action 2.3.2: Create target decks of ransomware developers, criminal affiliates, and ransomware variants.

To better operationalize and focus resources, the U.S. Government and the security community should work together to create prioritized target decks for ransomware developers, criminal affiliates, and ransomware variants based on how much harm they are doing and the breadth of their operations. The core of this effort must focus on unveiling the threat actors themselves and understanding their organization(s), with the goal of identifying vulnerabilities that can be exploited to disrupt the threat, using all capabilities available to the private industry and governments. This effort should include working more closely with the security community on a routine basis to share information and coordinate operations, to be facilitated by the JRTF and RTFH described in Action 1.2.2.

Timing: *6 to 12 months.* **Lead:** *U.S. Federal Government and international equivalents.*

Action 2.3.3: Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure.

Ransomware events are not singular, but part of an ongoing campaign of extortion against government and private-sector entities. Kill-chain analyses of ransomware organizations reveal a complex network of associates and entities. These organizations have been established to function as an extortion operation with repeatable outcomes. The various components of the organization include creators of malware, establishment of ransomware affiliates, franchise fees or percentage of ransomware payouts to the operation leaders, digital wallet creation, money laundering, using money mules, and more.

Law enforcement should disrupt the ransomware criminal enterprise by using established frameworks that have been applied successfully to disrupt the activities of the mafia and other criminal organizations. The U.S. government should leverage the power of the RICO statute, as called for above in Action 1.2.4, to prosecute ransomware criminals. The RICO statute (Title 18 USCS § 1962) serves as a "mafia business tax", and prohibits racketeering. RICO investigations provide influential tools to inspire cooperation of members and supporters of a criminal enterprise, such as enhanced prison terms for any conspirators, and forfeiture and exposure to civil RICO investigations. If deemed necessary, the federal government should undertake immediate action to ensure ransomware crimes are predicates for use of the RICO statutes.

Timing: *12 to 24 months.* **Lead:** *U.S. Law Enforcement and international equivalents.*

Goal #3

Help organizations prepare for ransomware attacks

Any organization can fall victim to ransomware, creating catastrophic disruption for the organization and those it serves. Yet despite extensive press coverage and content on this topic, the threat is poorly understood by many public- and private-sector leaders, and the majority of organizations lack an appropriate level of preparedness to defend against these attacks. Even firms that have invested in cybersecurity broadly may be unaware of how to prepare for, and defend specifically against, ransomware attacks, and information available is in many cases oversimplified or excessively complicated.

The challenge is to increase awareness and build defenses that will be effective both at scale and over time as the threat evolves. To do this, governments and industry leaders need to better connect with key audiences, including both the organizational leaders who need to understand that ransomware is a real and relevant threat to their organization, and also the individuals in operational roles (such as IT and security professionals) who need guidance on how to prioritize mitigation efforts given limited resources. Support should be customized based on each organization's current situation, including to what extent it is already appropriately informed and whether it has appropriately invested in time and resources.

Objective 3.1:
Support organizations with developing practical operational capabilities

Guides and technological tools to mitigate ransomware are currently available; however, many are insufficient, overly simplified, or too complicated, and the general level of noise surrounding this problem is confusing and problematic.

Action 3.1.1: Develop a clear, actionable framework for ransomware mitigation, response, and recovery.

Although multiple organizations have published ransomware guides, no single, authoritative source of best practices exists. The current state of awareness around ransomware is similar to the general environment prior to 2014, when no compilation of best practices existed for cybersecurity. At that time, the U.S. National Institute of Standards and Technology (NIST) led a multi-stakeholder process to develop the *Framework for Improving Critical Infrastructure Cybersecurity*. This framework has been widely adopted by organizations around the world and serves as a foundational cybersecurity risk management resource.

We have reached a similar point with the ransomware threat. The single most impactful measure that could be taken to help organizations prepare for and respond to ransomware attacks would be to create one internationally accepted framework that lays out clear, actionable steps to defend against, and recover from, ransomware.

Ransomware is a global problem, so governments and private-sector organizations around the world should collaborate on this effort to ensure the framework will work internationally. Efforts taken only in one jurisdiction may be regionally effective, but will likely push attackers to focus on different regions; a coordinated international effort will create greater long-term impact and more effectively disrupt the economics of the cybercrime market. It will also drive greater adoption in organizations that operate in more than one country.

As far as is practical, the framework should be consistent with existing cybersecurity frameworks, such as International Standards Organization publications[59] and the NIST Cybersecurity Framework,[60] but it should be specific to ransomware. It should build on the work that NIST's National Cybersecurity Center of Excellence has already done as part of the data integrity project and related papers. The framework should clearly identify each recommended action's impact, as well as the required investment of time and other resources. It should include multiple layers for different audiences; similar to the NIST Cybersecurity Framework, the top layer would be intended for executive decision makers, the second and third layers for operational managers, and the fourth layer for front-line implementers.

The ransomware-specific framework should also identify what approaches are most successful in dealing with ransomware and why. The framework should identify what constitutes a reasonable due diligence review prior to payment, consistent with actions 4.1.1 and 4.1.2, which address the creation of ransomware emergency response authorities and a ransomware response fund.

In addition, industry-specific profiles should be developed to tailor the Ransomware Framework to different industries or sectors. Creating different profiles for local governments, small- and medium-sized businesses, and large enterprises, for example, would enable different types of organizations to adapt the framework to their particular situations.

Timing: *12-24 months, and updated yearly thereafter.*
Lead: *NIST for the US, and international equivalents, with private-sector participation.*

Action 3.1.2:
Develop complementary materials to support widespread adoption of the Ransomware Framework.

Additional materials should be developed to accompany the ransomware prevention framework, drawing from existing resources, to further articulate how organizations can leverage specific security capabilities, technologies, and policies to meet the frameworks' identified best practices. Such materials could include:

- Detailed deployment toolkits and guides to assist specific sectors or market segments with applying the framework;
- Mappings to existing popular cybersecurity frameworks, e.g. NIST, ISOs, CIS controls
- A ransomware-specific risk assessment tool;
- Ransomware reference architectures (such as those developed by NIST's National Cybersecurity Center of Excellence);
- A ransomware killchain;
- A checklist to help organizations to hold managed service providers (MSPs) and IT vendors accountable.

Timing: *12-24 months, and updated regularly thereafter.* **Lead:** *NIST for the US, and other international equivalents.*

Action 3.1.3: Highlight available internet resources to decrease confusion and complexity.

Many decision aids exist to aid organizations preparing for, and responding to, ransomware attacks. While this volume of content is designed to help, it can in fact hinder preparedness or response as organizations struggle to identify the most relevant and actionable guidance for their situation. It is challenging for organizations to determine which guides can be trusted to provide high-quality, accurate advice. To address these shortcomings, the Task Force recommends a two-pronged approach.

First, internet search companies could take steps to make sorting through online materials easier. For example, during the COVID-19 pandemic, internet search companies took steps to highlight credible content related to the pandemic to make it easier to find the most up-to-date and relevant information, and also to minimize the negative impact of mis- or disinformation. A similar effort focused on ransomware would help IT and security professionals navigate this highly complex and evolving threat landscape, and quickly identify the most important information and guidance. Once the Ransomware Framework and complementary materials are published, these would be prioritized on these search pages.

Second, a nonprofit entity, such as the Cybercrime Support Network, should collect and maintain a reference library of decision aids and best practice guides for responding to a ransomware attack. This step would provide a vetted library of material for organizations to draw on to prepare for and/or respond to a ransomware attack.

Timing: *6-12 months for first iteration, and ongoing thereafter.*
Lead: *For curation, internet search companies. For aggregation, a nonprofit like the Cybercrime Support Network (CSN) could lead this process in the U.S., together with international partners.*

Objective 3.2:
Increase knowledge and prioritization among organizational leaders

There is a stark difference between being aware of ransomware as a threat and having a real understanding of the dynamics, mitigations, and potential impacts of an attack. Organizational leaders need greater understanding about the significance and relevance of the ransomware threat in order to allocate resources and prioritize focus.

Action 3.2.1: Develop business-level materials oriented toward organizational leaders.

Organizational leaders traditionally see security as niche and highly technical. They need to understand ransomware as a whole-organization event, in non-technical, business risk-relevant terms. While the Ransomware Framework described in Action 3.1.1 has a top layer aimed at executives, additional materials should highlight business needs and risks, and aim toward educating organizational leaders about the threat.

These materials should include a simplified and translated overview of the framework; a ransomware primer for business leaders; or a checklist for organizational leaders to address with operational staff. They could also include detailed case studies of real, anonymized attacks related to critical sectors, highlighting how ransomware attacks occurred and the resulting business impact. Any materials should also consider the regulatory landscape,

emphasizing how adhering to preparatory frameworks can reduce the likelihood of fines or other penalties.

Timing: *6-12 months, with updates yearly as needed.*
Lead: *CISA or equivalent international government agency tasked with capacity-building around cybersecurity.*

Action 3.2.2: Run nationwide, government-backed awareness campaigns and tabletop exercises.

A government-backed awareness campaign will not only help raise the profile of ransomware as a serious business issue, but it will also increase the credibility and need for focus among busy organizational leaders. This should be coordinated with efforts addressing operational technical roles. Such a campaign should leverage appropriate international organizations, state and local governmental entities, non-profits, and industry organizations and influencers. It should also be accompanied by tabletop exercises that provide opportunities for learning and collaboration.

Additionally, as many organizational leaders rely on trade or local business networks to learn about challenges facing organizations in their sector or region, we recommend engaging these organizations in awareness campaigns. In the United States, organizations that could be considered include Chambers of Commerce, the National Association of Corporate Directors, the Young Presidents' Organization, and various trade associations. These organizations may need funding in order to be able to take on a campaign of this significance.

Timing: *12-24 months years, and ongoing for as long as relevant.*
Lead: *U.S. Federal government and international equivalents, appropriate agency leads (e.g., Education or Homeland Security or equivalents), and key nonprofit partners.*

A Little Goes a Long Way

Increasing security in a few key areas could make a significant difference for organizations in their effort to prepare for ransomware attacks. Complex security software or complete network rebuilds may not be necessary. For example, as SecurityScorecard notes in a recent report, implementing multi-factor authentication or adopting password managers can dramatically improve an organization's security posture.[61] Although any organization, regardless of its security, can be a target for a ransomware attack, improving baseline security and raising awareness among employees can go far in protecting organizations from attack.

Tabletop Exercises

As part of an awareness-building campaign, national governments could lead multi-stakeholder "tabletop exercises" for states, cities, businesses, and international partners. Tabletop exercises bring together key stakeholders to use scenarios or simulations of ransomware events, and could help organizations hone internal and external organizational collaboration and response processes. Such exercises are valuable in helping organizations understand the importance of prioritizing ransomware preparedness, as well as their personal risks and responsibilities as part of a globally interconnected system. Regular exercises can also help build strong relationships and facilitate more robust ransomware threat information-sharing and incident response collaboration. As an example, the U.S. Department of Homeland Security conducts a bi-annual national cyber exercise called Cyber Storm.

Objective 3.3:
Update existing, or introduce new, cybersecurity regulations to address ransomware

Regulations and standards related to cybersecurity vary widely, and in most cases do not specifically address ransomware. Updating regulations and filling gaps with new regulations will help drive better adoption of ransomware mitigations in core regulated sectors.

For the new regulations proposed below, the government may want to consider a mechanism to address how quickly the technology and threat landscapes evolve, compared to the process for updating laws and regulations. For example, a private- or public-sector standards body (e.g. NIST, the Center for Internet Security, or a group similar to the Payment Card Industry Security Council) could set and annually update minimum required standards, and the law would incorporate this group's standards.

Action 3.3.1: Update cyber-hygiene regulations and standards.

Existing cybersecurity regulations — such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and the Directive on Security of Network and Information Systems (NIS) in the European Union, as well as non-regulatory standards such as the Payment Card Industry Data Security Standard (PCI DSS) — all set a baseline for cybersecurity in specific regulated sectors where protection of data and essential services is considered critical. Though some targeted guidance exists,[62] many standards do not specifically address ransomware, despite the significance of this threat. These and other existing cybersecurity regulations and standards should thus be reviewed and, where necessary, updated to incorporate measures that align with the recommended Ransomware Framework (see Action 3.1.1) to more directly mitigate ransomware attacks

Timing: *Dependent on the creation of the Ransomware Framework (Action 3.1.1); likely 12-24 months, with subsequent iterations in the long term (24+ months).*
Lead: *State and federal government(s) or equivalent law-making bodies, with support from state/local entities, think tanks, and nonprofits.*

Action 3.3.2: Require local governments to adopt limited baseline security measures.

Ransomware attacks impacting local governments are catastrophic not only for the organizations themselves, but also for the constituents they serve. Mandating certain behaviors and practices will help local governments better defend against attacks, and may help them provide enhanced support for small-to-medium-sized businesses operating in their jurisdiction. In the United States, required measures could include:

- Joining the Multi-State Information Sharing and Analysis Center (MS-ISAC);
- Signing up for the MS-ISAC's Malicious Domain Blocking and Reporting (MDBR),[63] unless already running a comparable DNS filtering service; and
- Signing up for CISA's infrastructure and web application scanning services.[64]

Other measures could include the MS-ISAC offering ransomware-specific training and support to cities, though any additional requirements would likely require funding or financial incentives.

Timing: *6-12 months, and updated yearly thereafter.*
Lead: *U.S. Federal Government and international equivalents.*

Action 3.3.3:
Require managed service providers to adopt and provide baseline security measures.

Managed service providers (MSPs) often cover the IT and security functions for organizations that cannot invest in in-house expertise and technologies. MSPs do not commonly provide extensive security coverage or ransomware mitigations, but doing so would likely create widespread positive impact for small-to-medium-sized organizations. Baseline security measures for MSPs could include:

- Adherence with a cyber-hygiene program (for example, CIS Controls Implementation Group 1[65] and the NIST Cybersecurity Framework;[66]
- Mandatory disclosure across the MSP's customer base if there is a ransomware incident involving the MSP's service offering; and
- Forming an MSP-ISAC, an information sharing and analysis center specific to this industry.

Note that some funding or financial incentivization may initially be needed to help MSPs develop cybersecurity capabilities.

Timing: *6-12 months.* **Lead:** *U.S. Congress and international equivalent lawmakers.*

Objective 3.4:
Financially incentivize adoption of ransomware mitigations

Many organizations are under-invested in cybersecurity and resilience, and may lack the resources to manage the ransomware threat. By providing financial incentives, governments can help the most vulnerable and resource-constrained organizations tackle this issue. For some organizations, incentives may be the only means available to prepare for, and defend against, a ransomware attack.

Action 3.4.1: Highlight ransomware as a priority in existing funding provisions.

Where grants or funding are already offered and may be used for cybersecurity activity, we recommend that the accompanying language should be updated to highlight ransomware preparedness as a priority for spending and focus.

According to a Third Way paper on U.S. federal grants for cybersecurity,[67] eight existing preparedness grants are available to state, local, tribal, and territorial (SLTT) governments, transportation authorities, nonprofits, and private entities through the Federal Emergency Management Agency (FEMA). These have recently been changed to allow recipients to spend funds on cybersecurity, as when FEMA identified cybersecurity as a "priority area" in 2018 for the largest DHS preparedness grant, and required fund recipients to spend at least 5% of their funds on cybersecurity for critical infrastructure. This prioritization and funding expansion should continue across additional grants and should specifically highlight ransomware preparedness as an urgent priority.

Timing: *3-6 months.* **Lead:** *Relevant fund designation agencies.*

Action 3.4.2: Expand Homeland Security Preparedness Grants to encompass cybersecurity threats.

Under current law, Homeland Security Preparedness Grants focus on terrorism. Given the threat that ransomware poses to U.S. state, local, tribal, and territorial government entities, expanding this grant program to encompass cybersecurity threats would provide tremendous benefits. In addition to making SLTTs more resilient to ransomware, these investments will likely improve service delivery as upgrading software and hardware is often the most cost-effective security investment an organization can make. As noted in Action 3.4.3, access to these grants should be conditioned upon demonstrated alignment with the Ransomware Framework after it is developed.

Timing: *6-12 months.* **Lead:** *Department of Homeland Security, working with Congress.*

Action 3.4.3: Offer local government, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework.

In 2018, the U.S. Congress's Help America Vote Act (HAVA) allocated grant funds to help states bolster their election security. A similar model, through which states manage the delivery of grant funds to municipalities, could be employed to provide grants as financial incentives for demonstrated alignment with the Ransomware Framework. This could help motivate U.S. State, Local, Tribal, and Territorial government entities (SLTTs) to better prepare for and defend themselves against a ransomware attack. Continued provision of such grants should be based on clear measures of progress and advancement toward self-reliance. A similar model could be investigated for suitability in other countries.

Timing: *Dependent on the creation of the Ransomware Framework in Action 3.1.1; likely 12-24 months.*
Lead: *U.S. Federal government and international equivalents.*

Action 3.4.4: Alleviate fines for critical infrastructure entities that align with the Ransomware Framework.

A recent amendment to the HITECH ACT[68] requires the U.S. Department of Health and Human Services, when considering whether an entity should be fined for a HIPAA Security Rule-related violation, to consider the extent to which the entity has demonstrated alignment to an established risk management framework. A similar model could apply to other regulated critical infrastructure sectors to strongly incentivize adherence to established risk management frameworks for ransomware prevention.

Timing: *12-24 months.* **Lead:** *U.S. Federal government and international equivalents.*

Action 3.4.5: Investigate tax breaks as an incentive for organizations to adopt secure IT services.

Governments should offer tax breaks or other financial incentives to businesses that meet certain baseline standards for ransomware preparedness, as laid out in the Ransomware Framework under Action 3.1.1. Such a program should be structured to ensure long-term self-reliance. Leveraging tax breaks could help drive adoption of best practices for preparation for ransomware attacks; however, there are many practical considerations around who would qualify, whether the savings would offset costs, and how organizations would prove their qualification.

.**Timing:** *24 months.*
Lead: *U.S. Federal government and international equivalents.*

Goal #4

Respond to ransomware attacks more effectively

For victim organizations, a ransomware attack can be a stressful, potentially existential event. Crucial decisions about how to respond — including whether to pay the ransom — must be made under intense pressure. Facing the potential threat of losing their data permanently, organizations may make hurried decisions, particularly if they lack understanding about the ramifications of paying a ransom or the full range of alternatives open to them.

In order to improve organizations' ability to respond to ransomware attacks more effectively, government and industry leaders should increase the resources and information available to ransomware victims. At the same time, governments should require organizations to take certain actions before paying a ransom, including reporting the payment to the government. Ultimately, increased support for ransomware victims, including improved awareness of legal requirements prior to payment, will decrease the number of organizations that feel compelled or trapped into paying ransoms.

Objective 4.1:
Increase support for ransomware victims

Ransomware can severely disrupt an organization's business operations, and remediation efforts can take a long time. The resulting revenue loss can prove untenable for many companies, and can be a major crisis for hospitals and other critical infrastructure. Further, for many local governments and small- and medium-sized businesses, the cost of rebuilding networks to avoid paying the ransom is prohibitively expensive. A platform of support resources should be established and made available to help ransomware victims with the recovery process.

Action 4.1.1: Create ransomware emergency response authorities.

Ransomware attacks that have widespread, disruptive effects across society often fall outside the scope of traditional disaster response authorities. To address this gap, national governments should create special authorities to mitigate the effects of ransomware attacks that have impacts beyond the affected organization. The Cyberspace Solarium Commission recommended creating the authority to declare a "cyber disaster."[69] The Ransomware Task Force supports this idea and recommends that it should explicitly cover ransomware incidents.

A cyber-disaster authority would enable federal agencies to assist victim organizations and local governments, as well as make other resources available, such as incident response support and forensic analysis. Such actions should be limited to dealing with the immediate crisis and not long-term, ongoing engagement. To enable such

"cyber disaster declarations," Congress could choose to amend the primary law governing natural disaster response activities, typically referred to as the Stafford Act, to explicitly cover cyber incidents, or it could create a new, separate authority.

Timing: *12-24 months.* **Lead:** *U.S. Federal government, and international equivalents.*

Action 4.1.2: Create a Ransomware Response Fund to support victims in refusing to make ransomware payments.

While a company might determine that paying a ransom is economically rational, such a decision supports the criminal enterprise and is rarely in the public interest. To enable more companies to bear the financial cost of remediation, national governments should create "Cyber Response and Recovery Funds" (CRRFs). In addition to other goals, a CRRF should cover restoring IT functionality for local governments, critical national functions, or other entities as they recover from a ransomware attack, particularly when those entities lack access to appropriate cyber insurance or when a cyber insurance policy does not cover the event. This approach would be similar to the Terrorism Risk Insurance Program, which "provides for a transparent system of shared public and private compensation for certain insured losses resulting from a certified act of terrorism."[70] If such funding were available for ransomware victims, then cost would play a smaller role in an organization's decision about whether to pay the ransom. As an incentive to invest in cybersecurity, governments could consider requiring the organization to cover some portion of the ransom as a "deductible." Governments could also consider additional requirements to access the fund, such as demonstrating use of the Ransomware Framework in Action 3.1.1, to raise organizations' overall level of cybersecurity.

Timing: *12-24 months.* **Lead:** *U.S. Federal government in consultation with the insurance industry, and international equivalents.*

Action 4.1.3: Increase government resources available to help the private sector respond to ransomware attacks.

Many organizations will seek government assistance during a ransomware attack. In the United States, the Treasury Department's guidance on ransomware payments essentially requires organizations to consult with the Department if they want to pay the ransom. However, in many countries, agencies cannot fully meet their mandates with existing resources, nor is it always clear which agency has the responsibility or capability to address an inquiry.

Therefore, governments should increase funding for agencies to respond to ransomware-related inquiries so they can meet demand, through a combination of additional staff and improved technology. In addition, in the U.S. context, the Department of Homeland Security's CISA should consider providing a concierge or ombudsman service for private-sector entities seeking guidance on ransomware-related questions. Under this approach, CISA would not be responsible for interpreting another agency's guidance, but it would direct the inquiry to the correct office within the Federal government. This assistance would facilitate better decision-making within the private sector.

For example, the U.S. Treasury Department has indicated that ransom payments could violate sanctions against certain individuals or organizations. Treasury's guidance also indicates that organizations can be held strictly liable for such payments, which means they can be punished for sanctions violations, even if they were unaware

or unable to determine that the recipient is on a prohibited list. As a result, many organizations will want to know whether a potential payment recipient is a sanctioned entity. Given the volume of potential ransomware payments, the Treasury will likely need additional resources to meet demands from the private sector. Second, inquiries may not initially go to the Treasury; CISA could ensure that inquiries it receives regarding Treasury guidance get routed to the correct office.

Timing: *12-24 months*. **Lead:** *U.S. Federal government, and international equivalents*.

Action 4.1.4: Clarify United States Treasury guidance regarding ransomware payments.

In October 2020, the United States Treasury Department's Office of Foreign Assets Control (OFAC) issued an advisory to companies providing services to ransomware victims. This advisory indicates that OFAC will consider ransomware payments as a sanctions violation if the recipient is on the Specially Designated Nationals and Blocked Persons List (SDN List), another blocked person, or covered by comprehensive country or region embargoes. Additionally, the advisory states that a violation by a non-U.S. person that causes a U.S. person to violate any sanctions, or U.S. persons facilitating actions of non-U.S. persons in an effort to avoid U.S. sanctions regulations, are also prohibited. Finally, the advisory notes that any penalties could be assessed under strict liability, which means even if an organization did not know that paying the recipient would constitute a sanctions violation, they can still be held liable for the action.

While this guidance may seem straightforward, Task Force members who have specifically worked within this regime made the point that identifying payment recipients can prove quite challenging, especially under the short timelines of a ransomware attack. Even if an organization asks OFAC whether a particular recipient falls into a prohibited category or seeks a payment license, OFAC is not resourced to provide answers rapidly enough for a company facing tight extortion timelines. Experts have identified other unanswered questions with the advisory. While the Task Force supports Treasury's goal of reducing payments to criminals and in particular to prohibited entities, the advisory does not provide sufficient detail to be effective in achieving this outcome.

Therefore, the Task Force recommends that the U.S. Treasury Department issue additional clarifying guidance to supplement this advisory. This clarifying guidance should address such issues as what constitutes due diligence in determining the payment recipient's identity, the liability OFAC would assign to each stakeholder, the timeline and process for obtaining a payment license (should an organization choose to pursue that route), and to what extent OFAC would consider the harms to people serviced by a ransomware victim in determining whether to grant a license, if required. Taking into consideration the OFAC Advisory, as well as the almost simultaneous Financial Crimes Enforcement Network (FinCEN) Advisory and the Department of Justice Framework issued in October 2020, OFAC should coordinate with these government counterparts to ensure the clarification considers their goals and incorporates them into OFAC's response to this request for clarification.

Timing: *6-12 months*. **Lead:** *U.S. Treasury Department. During the update process, the Treasury Department should consult with relevant industry, academia, civil society, and cybersecurity experts.*

Objective 4.2:
Increase the quality and volume of information about ransomware incidents

While everyone agrees that ransomware is a significant problem, there is a lack of reliable, representative data about ransomware's scope and scale. Further, information about ongoing ransomware threats does not yet reach as much of the digital ecosystem as it should – to include both across sectors of private industry or within responsible governmental departments and agencies. Therefore, improving the quality and volume of ransomware information would enable better deterrence, enhance preparedness, and inform disruption activities.

Action 4.2.1: Establish a Ransomware Incident Response Network (RIRN).

To increase the flow of ransomware information, a wide array of public and private organizations should formally agree to share such information rapidly and in standardized formats. To implement this action, the Task Force recommends the creation of the Ransomware Incident Response Network (RIRN). The RIRN would serve several functions, including facilitating receipt and sharing of incident reports, directing organizations to ransomware incident response services, aggregating data, and sharing or issuing alerts about ongoing threats. Not all entities within the RIRN would participate in all RIRN functions. For example, some RIRN organizations might not accept individual incident reports or conduct incident response activities, but they could refer inquiries to another RIRN organization that would.

RIRN entities engaged in the receipt and sharing of specific incident reports would agree to receive and share reports using the standard format developed under 4.2.2; adopt a system of unique identifiers to avoid double-counts while maintaining anonymity; and share the resulting information in an anonymized form with other cyber intelligence organizations and national governments in the network, including law enforcement. RIRN organizations would also agree to direct reporting entities to available public and private resources, including incident responders that could assist the entity through the ransomware attack. The RIRN should consider whether to enable organizations to report anonymously, such that the receiving organization does not know the identity of the submitter.

Other RIRN functions could include sharing or issuing alerts about ransomware threats in non-technical language. Such alerts would be designed to engage as broad an audience as possible and to prompt action to counter specific threats.

The RIRN network should include non-profit organizations, such as the Cybercrime Support Network, Cyber Readiness Institute, Global Resilience Federation, Global Cyber Alliance, Information Sharing and Analysis Organizations, and Cyber Threat Alliance; for-profit entities, including cybersecurity vendors, insurance providers, and incident responders; and national government agencies, including law enforcement.

Timing: *12-24 months to reach full operational capability.* **Lead:** *A nonprofit and international equivalents.*

Action 4.2.2: Create a standard format for ransomware incident reporting.

Different organizations require different types of information about ransomware attacks to serve a variety of goals. Cybersecurity providers need technical data about the malware used in the attack to build protections for other customers, while law enforcement may be interested in other information, such as the wallet number and ransom note. At the same time, reporting can be a significant burden to an organization suffering a ransomware attack.

In order to reduce the burden of ransomware reporting while increasing its utility for recipients, a standard ransomware incident report format should be developed through a multi-stakeholder process. Any organization reporting a ransomware incident or reporting on behalf of another organization could use this format. The format should encompass both non-technical information (such as affected organization type or ransom amount) and technical information (such as indicators of compromise). It should also leverage existing formats, such as STIX[71] and the MITRE ATT&CK[72] framework for technical data and suspicious activity reports, to make integration across reporting systems as easy as possible. The required fields should be kept to a minimum, but the format should enable more technically capable reporting entities to include more detailed information. Creating such a standard format would also make aggregating and anonymizing reports easier.

Timing: *6-12 months.* **Lead:** *A nonprofit, such as the Institute for Security & Technology or the Cyber Threat Alliance, and international equivalents.*

Action 4.2.3: Encourage organizations to report ransomware incidents.

National governments should encourage organizations that experience a ransomware attack to report the incident to the RIRN using the common format. This encouragement could take the form of the "See Something, Say Something" campaign, and would note the benefits of reporting, the low level of effort required, and the protections built into the reporting process (for example, that reports can be made anonymously). The government should use different outreach methods for different parts of the ecosystem, for example, using tailored outreach for K-12 engagement versus engagement with the manufacturing sector.

Timing: *6-12 months, updated ongoing as needed.*
Lead: *Government cybersecurity agency or cyber center; DHS CISA in the U.S., with support from relevant government, industry, academia, civil society ransomware experts to craft the message.*

Action 4.2.4: Require organizations and incident response entities to share ransomware payment information with a national government prior to payment.

In the US, 54 states and territories have breach disclosure laws, and many sectors also have federal reporting requirements, such as the Gramm-Leach-Bliley Act (in the financial sector) and Sarbanes-Oxley (for publicly traded companies). In the European Union, the Directive on Security of Network and Information Systems (NIS Directive) requires essential entities to report data breaches. Updating breach disclosure laws to include a ransom payment disclosure requirement would help increase the understanding of the scope and scale of the crime, allow for better estimates of the societal impact of these payments, and enable better targeting of disruption activities. Further, requiring ransomware victims to report details about the incident prior to paying the ransom would enable national governments to take actions such as issuing a freeze letter to cryptocurrency exchanges, as called for in Action 2.1.4. Finally, publishing summaries of the information reported under this requirement will help organizations understand how preparative measures need to adapt as attacks evolve.

This mandate should require organizations to report directly to a non-regulatory government agency. In turn, a receiving agency should share the reported information with other appropriate, non-regulatory government agencies as rapidly as possible and, after appropriate anonymization, to the RIRN. To reduce the burden on victim organizations, the mandatory report should only encompass limited information, such as ransom date, demand, payment instructions (e.g., wallet number and transaction hashes), and amount, and it should use the standard reporting format developed through Action 4.2.2. However, the reporting process should allow organizations to provide additional technical information about the incident when they can, and use insurance providers or incident response entities to report on their behalf. In order to avoid forcing organizations to put themselves in potential regulatory jeopardy, the reporting requirement should incorporate limited liability protections, including that the report cannot form the basis for a regulatory or other enforcement action. When enacting this mandate, governments should consider appropriate penalties for organizations that do not comply with the requirement.

Timing: *12-24 months.* **Lead:** *U.S. Federal government, and international equivalents.*

Objective 4.3:
Require organizations to consider alternatives to paying ransoms

While most leaders oppose the idea of paying ransoms and only reluctantly agree to make a payment, they may arrive at the decision based on limited information. A common misperception is that the only alternative to payment is entirely rebuilding the network; that option might be prohibitively costly or take too long for organizations that have critical services that need immediate restoration. However, in many cases, viable alternatives exist between payment and a full network rebuild, such as restoring data from unencrypted shadow copies. Finally, a small minority of organizations might assume that paying the ransom will be the easiest path to restoring operations and may not otherwise review their alternatives.

Requiring organizations to analyze options before paying ransoms could enable more organizations to choose alternative paths. However, even if governments choose not to make these recommendations mandatory, they should still be incorporated as best practices in the Ransomware Framework developed under Action 3.1.1.

Action 4.3.1: Require organizations to review alternatives before making payments.

Although ransomware attackers often try to use time pressure to try to persuade victims to pay, often other options are available. Unencrypted shadow copies of data might be accessible, allowing a victim to recover their business operations, or a decryption key might exist for that particular ransomware. If ransomware victims have a legal requirement to conduct a due diligence review before making a payment, then they would have the ability to push back on demands for immediate payment. This review would also reveal whether options between payment and rebuilding the network from scratch are viable. For example, the mandate could require organizations to consult with initiatives like No More Ransom to determine if their information can be decrypted without paying.

Such reviews should be scaled to the size and criticality of the organization; for SMBs, the review might only consist of two or three actions. If more organizations actively seek alternatives to payment, fewer will feel

compelled to pay. National governments should enact a legal requirement for conducting the review; in the U.S. context, the private sector should develop what constitutes the due diligence review as part of the cost-benefit analysis matrix in Action 4.3.3.

Timing: *12-24 months.* **Lead:** *U.S. Federal government and international equivalents.*

Action 4.3.2: Require organizations to conduct a cost-benefit assessment prior to making a ransom payment.

In addition to searching for payment alternatives, organizations should also compare the costs of paying the ransom with those of not paying. Given the complexities involved, the costs associated with either option are not necessarily obvious without analysis. Many costs will be incurred regardless of whether or not an organization pays the ransom; for example, a company will be liable for breach notification costs regardless of whether the attacker upholds their promise not to further release the data if the ransom is paid. Consequently, such costs should not factor into the decision. In many cases, the analysis could show that paying the ransom is not in fact the cheaper option.

The Task Force recommends that national governments require organizations to conduct a cost-benefit analysis prior to making a ransom payment. Such statutes could also require medium- to large enterprises to document this cost-benefit analysis prior to making a payment or authorizing their insurance provider to make a payment on their behalf. Once a standard cost-benefit analysis matrix is developed, as called for in Action 4.3.3, governments could require the use of the standard matrix to facilitate inter-organization comparisons and data collection.

Timing: *12-24 months Lead.* **Lead:** *U.S. Federal government and international equivalents.*

Action 4.3.3: Develop a standard cost-benefit analysis matrix.

As noted in 4.3.2, analyzing the costs associated with a payment decision can prove challenging. Many organizations would benefit from having a standard analytic matrix to carry out this task. However, most existing decision guides do not explicitly tackle this question and clearly lay out the various cost factors. Therefore, the Task Force recommends that the Ransomware Framework called for in Action 3.1.1 specifically include a cost-benefit matrix. This matrix should enable organizations to identify the costs associated with not paying compared to the costs of paying the ransom, as well as which costs to exclude from the analysis because they are incurred in either case.

Timing: *12-24 months.* **Lead:** *NIST for the US, and international equivalents, with private sector participation*

A Note on Prohibiting Ransomware Payments

The question of whether to prohibit payment of ransoms has become increasingly pressing, and was raised by every working group in the Task Force. The argument in favor of a ransom ban holds that ransomware is primarily motivated by profit, and if the potential for a payout is removed, attackers will shift away from this tactic. A further argument is that ransom profits are used to fund other, more pernicious crime, such as human trafficking, child exploitation, terrorism, and creation of weapons of mass destruction. When viewed with that lens, the case for prohibiting payments is clear.

The challenge comes in determining how to make such a measure practical, as there remains a lack of organizational cybersecurity maturity across sectors, sizes of organization, and geographies. Ransomware attackers require little risk or effort to launch attacks, so a prohibition on ransom payments would not necessarily lead them to move into other areas. Rather, they would likely continue to mount attacks and test the resolve of both victim organizations and their regulatory authorities. To apply additional pressure, they would target organizations considered more essential to society, such as healthcare providers, local governments, and other custodians of critical infrastructure.

Were a government to take a hardline approach on non-payment, perhaps even offering to shore up victims in their jurisdiction in some manner, attackers will look for other potential targets before moving to new sources of revenue. This means they will focus on countries or sectors where governments have not implemented the same policy or are unable to provide a safety net for victims. Even in jurisdictions that offer support for critical entities, organizations that do not qualify for this support may instead pay the ransom without disclosing the incident. This could then open them to further extortion.

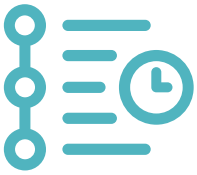
As such, any intent to prohibit payments must first consider how to build organizational cybersecurity maturity, and how to provide an appropriate backstop to enable organizations to weather the initial period of extreme testing. Ideally, such an approach would also be coordinated internationally to avoid giving ransomware attackers other avenues to pursue.

With all these pragmatic considerations in mind, the Ransomware Task Force did not reach consensus on prohibiting ransom payments, though we do agree that payments should be discouraged as far as possible. We recognize, though, that some governments may want to pursue ransomware payment prohibitions based on their policy judgments. Given the potential consequences, the Task Force has identified three factors that governments should consider to reduce the negative impacts of such prohibitions:

Factors to Consider before Pursuing a Ransomware Payment Prohibition

1

Timeline



Governments and organizations need time to adapt to such a dramatic change in the law, so prohibitions cannot be enacted immediately. For example, governments need time to set up victim protection and support programs, as detailed below. Insurance companies need time to update policies to reflect the payment prohibition. The payment facilitator ecosystem would need time to shut down operations in an orderly fashion. Thus, a prohibition statute should establish milestones or conditions that would need to be met before the prohibition would go into effect.

2

Phasing

Prohibitions should be implemented in a phased manner, potentially over a matter of years. Phasing could be based on sector: for example, a prohibition could be enacted on public entities before it is extended to the private sector.

3

Victim Protection and Support

To help offset the potential burden on victims, governments should provide strong protection and support policies. Examples of such policies include the Cyber Response and Recovery Fund,[73] which could be used to help cover business continuity and remediation costs for organizations attacked with ransomware; establish rapid response teams to assist life-line organizations (such as hospitals) to restore functionality quickly; and provide liability protection for business interruptions caused by refusing to pay ransoms.

Conclusion

The Ransomware Task Force developed the recommendations outlined in this report to provide a multi-pronged approach to countering ransomware, and it will be crucial for organizations across sectors to work together and act immediately to tackle this challenge. Make no mistake: reducing the ransomware threat will not be easy, and it will not be accomplished by any individual government or organization alone; this effort will require coordination, collaboration, and investment of time and resources.

The persistence of safe harbors and the challenge of tracing transactions through cryptocurrencies, combined with the complexity of attribution and prosecution, stack the odds in ransomware criminals' favor. The old adage that a cybercriminal only has to be lucky once, while a defender has to be lucky every minute of every day, has never been more true. Without major intervention, the situation will only get worse as ransomware criminals continue to evolve their tactics and the proliferation of devices through the "internet of things" dramatically expands the attack surface. The ever-more lucrative ransomware industry will draw in more threat actors, compounding the problem.

Adding to the challenge, victims of ransomware attacks may increasingly worry about reputational harm and be wary of disclosing details to the public. It is also likely that, as efforts to reduce ransomware become more successful, actors may choose to target increasingly critical systems and networks, and adopt techniques that are more aggressive in order to combat increased defenses or payment obstruction techniques.

Yet failing to act is not an option. Allowing the ransomware challenge to go unchecked could have disastrous consequences. Ransomware actors will only become more malicious, and worsening attacks will inevitably impact critical infrastructure, including communications, transportation, health and safety, distribution and logistics, utilities, and other critical infrastructure. Future attacks could easily combine techniques in ways that cause the infections to spread beyond their intended targets, potentially leading to far-reaching consequences, including loss of life.

The good news is that many of the recommendations outlined in this report may help improve organizations' cybersecurity broadly, and lead to the establishment of new collaborations dedicated to keeping our digital society safe. Indeed, we are still at the dawn of the digital age, and finding new ways to address ransomware and other cyber threats will have benefits that last for decades to come.

Summary of Recommendations

GOAL #1:	**Deter ransomware attacks through a nationally and internationally coordinated, comprehensive strategy**
Objective 1.1:	**Signal that ransomware is an international diplomatic and enforcement priority**
Action 1.1.1:	*Issue declarative policy through coordinated international diplomatic declarations that ransomware is an enforcement priority*
Action 1.1.2:	*Establish an international coalition to combat ransomware criminals*
Action 1.1.3:	*Create a global network of ransomware investigation hubs*
Action 1.1.4:	*Convey the international priority of collective action on ransomware via sustained communications by national-leaders*
Objective 1.2:	**Advance a comprehensive, whole-of-U.S. government strategy for reducing ransomware attacks, led by the White House**
Action 1.2.1:	*Establish an Interagency Working Group for ransomware*
Action 1.2.2:	*Establish an operationally focused U.S. Government Joint Ransomware Task Force (JRTF) to collaborate with a private-sector Ransomware Threat Focus Hub*
Action 1.2.3:	*Conduct a sustained, aggressive, public-private collaborative anti-ransomware campaign*
Action 1.2.4:	*Make ransomware attacks an investigation and prosecution priority, and communicate this directive internally and to the public*
Action 1.2.5:	*Raise the priority of ransomware within the U.S. Intelligence Community, and designate it as a national security threat*
Action 1.2.6:	*Develop an international-version of an Intelligence Community Assessment (ICA) on ransomware actors to support international collaborative anti-ransomware campaigns*
Objective 1.3:	**Substantially reduce safe havens where ransomware actors currently operate with impunity**
Action 1.3.1:	*Exert pressure on nations that are complicit or refuse to take action*
Action 1.3.2:	*Incentivize cooperation and proactive action in resource-constrained countries*

GOAL #2:	**Disrupt the ransomware business model and decrease criminal profits**
Objective 2.1:	**Disrupt the system that facilitates the payment of ransoms**
Action 2.1.1:	*Develop new levers for voluntary sharing of cryptocurrency payment indicators*
Action 2.1.2:	*Require cryptocurrency exchanges, crypto kiosks, and over-the-counter (OTC) trading "desks" to comply with existing laws*
Action 2.1.3:	*Incentivize voluntary information sharing between cryptocurrency entities and law enforcement*
Action 2.1.4:	*Centralize expertise in cryptocurrency seizure, and scale criminal seizure processes*
Action 2.1.5:	*Improve civil recovery and asset forfeiture processes by kickstarting insurer subrogation*
Action 2.1.6:	*Launch a public campaign tying ransomware tips to existing anti-money laundering whistleblower award programs*
Action 2.1.7:	*Establish an insurance-sector consortium to share ransomware loss data and accelerate best practices around insurance underwriting and risk management*

Objective 2.2:	**Target the infrastructure used by ransomware criminals**
Action 2.2.1:	*Leverage the global network of ransomware investigation hubs*
Action 2.2.2:	*Clarify lawful defensive measures that private-sector actors can take when countering ransomware*
Objective 2.3:	**Disrupt the threat actors, including ransomware developers, criminal affiliates, and ransomware variants**
Action 2.3.1:	*Increase government sharing of ransomware intelligence*
Action 2.3.2:	*Create target decks of ransomware developers, criminal affiliates, and ransomware variants*
Action 2.3.3:	*Apply strategies for combating organized crime syndicates to counter ransomware developers, criminal affiliates, and supporting payment distribution infrastructure*

GOAL #3: Help organizations prepare for ransomware attacks	
Objective 3.1:	**Support organizations with developing practical operational capabilities**
Action 3.1.1:	*Develop a clear, actionable framework for ransomware mitigation, response, and recovery*
Action 3.1.2:	*Develop complementary materials to support widespread adoption of the Ransomware Framework*
Action 3.1.3:	*Highlight available internet resources to decrease confusion and complexity*
Objective 3.2:	**Increase knowledge and prioritization among organizational leaders**
Action 3.2.1:	*Develop business-level materials oriented toward organizational leaders*
Action 3.2.2:	*Run nation-wide, government-backed awareness campaigns and tabletop exercises*
Objective 3.3:	**Update existing, or introduce new, cybersecurity regulations to address ransomware**
Action 3.3.1:	*Update cyber hygiene regulations and standards*
Action 3.3.2:	*Require local governments to adopt limited baseline security measures*
Action 3.3.3:	*Require managed service providers to adopt and provide baseline security measures*
Objective 3.4:	**Financially incentivize adoption of ransomware mitigations**
Action 3.4.1:	*Highlight ransomware as a priority in existing funding provisions*
Action 3.4.2:	*Expand Homeland Security Preparedness grants to encompass cybersecurity threats*
Action 3.4.3:	*Offer local governments, SLTTs, and critical NGOs conditional access to grant funding for compliance with the Ransomware Framework*
Action 3.4.4:	*Alleviate fines for critical infrastructure entities that align with the Ransomware Framework*
Action 3.4.5:	*Investigate tax breaks as an incentive for organizations to adopt secure IT services*

Goal #4:	Respond to ransomware attacks more effectively
Objective 4.1:	**Increase support for ransomware victims**
Action 4.1.1:	*Create ransomware emergency response authorities*
Action 4.1.2:	*Create a Ransomware Response Fund to support victims in refusing to make ransomware payments*
Action 4.1.3:	*Increase government resources available to help the private sector respond to ransomware attacks*
Action 4.1.4:	*Clarify U.S. Treasury guidance regarding ransomware payments*
Objective 4.2:	**Increase the quality and volume of information about ransomware incidents**
Action 4.2.1:	*Establish a Ransomware Incident Response Network (RIRN)*
Action 4.2.2:	*Create a standard format for ransomware incident reporting*
Action 4.2.3:	*Encourage organizations to report ransomware incidents*
Action 4.2.4:	*Require organizations and incident response entities to share ransomware payment information with a national government prior to payment*
Objective 4.3:	**Require organizations to consider alternatives to paying ransoms**
Action 4.3.1:	*Require organizations to review alternatives before making payments*
Action 4.3.2:	*Require organizations to conduct a cost-benefit assessment prior to making a ransom payment*
Action 4.3.3:	*Develop a standard cost-benefit analysis matrix*

Acknowledgements

The Institute for Security and Technology is incredibly grateful to the phenomenal group of volunteer experts that came together to make this effort a success. The communities that operate day in and day out to grapple with challenges like ransomware comprise countless unsung heroes, and we are lucky to have been able to convene such a diverse and expansive group of dedicated professionals. They graciously shared considerable amounts of their very limited time to provide their expertise and work through proposed solutions as part of the three-month sprint of the Ransomware Task Force. All of this took place during a period of significant high-level responsibilities across the industry.

Our effort consisted of four main working groups, with an additional three special projects teams, supplemented by numerous sub-working groups focused on everything from cryptocurrencies to "pizza parties" to cyber insurance. The Task Force consisted of members from civil society, private industry (from a range of sectors, including finance, cybersecurity, insurance, healthcare, and high technology), as well as members of government agencies from the United States and around the world.

We want to say a particular word of thanks to the RTF Working Group Co-Chairs, who poured an extraordinary amount of time and energy into organizing and leading large groups of experts, facilitating what were often lively and healthy debates, developing and formulating complicated recommendations, and lending their own extensive knowledge to the entire project. Their leadership elevated the process and this resulting report, and we cannot thank them enough.

We would also like to thank the many members of the Ransomware Task Force and their organizations, which afforded them the opportunity during otherwise exceedingly demanding times. They answered this call to action with dedication and their substantial expertise. We appreciate the resources that each of them brought to the table and the professional connections they have tapped into in order to move the process along and thoroughly vet our proposed solutions.

Lastly, we would like to thank the many unnamed people outside of the Task Force who answered our many questions, discussed ideas, and gave feedback on our recommendations.

We believe the recommendations in this report, if undertaken together and with alacrity, could lead to real change in the trajectory of this threat. All of this has been made possible by the dedication and care of this incredible group of people.

On behalf of all of us at the Institute for Security and Technology, a sincere thank you.

Note: *RTF Members and Working Group Members volunteered their time, and contributed to the report in working groups focused on specific problem sets. The resulting suite of recommendations in this document is a combination of all working group efforts, and each recommendation may not necessarily reflect the views of every participant.*

RTF Co-Chairs

Megan Stifel, *Global Cyber Alliance*

John Davis, *Palo Alto Networks*

Michael Phillips, *Resilience*

Executive Director
Philip Reiner, *Institute for Security and Technology*

RTF Working Group Co-Chairs

John Davis, *Palo Alto Networks*

Megan Stifel, *Global Cyber Alliance*

Michael Phillips, *Resilience*

Kemba Walden, *Microsoft*

Jen Ellis, *Rapid7*

Chris Painter, *The Global Forum on Cyber Expertise Foundation Board*

Michael Daniel, *Cyber Threat Alliance*

Philip Reiner, *Institute for Security and Technology*

RTF Staff

Sarah Powazek, *RTF Program Manager, Institute for Security and Technology*

Alexander Riabov, *Communications Manager, IST*

Leah Walker, *Future Digital Security Leader Fellow, IST*

Chuck Kapelke, *Writing Support*

Kathryn Pledger, *Pledger Designs*

Emma Hollingsworth, *Global Cyber Alliance*

RTF Membership

Joel de la Garza, *a16z*

Temi Adebambo, *Amazon Web Services*

David Forcsey, *Aspen Digital*

Jeff Troy, *Aviation ISAC*

Rich Friedberg, *Blackbaud*

Austin Berglas, *BlueVoyant*

Lewis Robinson, *Center for Internet Security*

Roger Francis, *CFC Underwriting*

Don Spies, *Chainalysis*

Pamela Clegg, *CipherTrace*

Brad Garnett, *Cisco*

Matt Olney, *Cisco*

Peter Lefkowitz, *Citrix*

Bill Siegal, *Coveware*

James Perry, *CrowdStrike*

Stéphane Duguin, *The CyberPeace Institute*

Yonatan Striem-Amit, *Cybereason*

Neil Jenkins, *Cyber Threat Alliance*

Andy Thompson, *CyberArk*

Ari Schwartz, *Cybersecurity Coalition*

John Banghart, *Cybersecurity Coalition*

Ryan Weeks, *Datto*

Patrice Drake, *Deloitte*

Keith Mularski, *Ernst & Young*

Stacy O'Mara, *FireEye*

Nick Bennett, *FireEye*

Jill Fraser, *Jefferson County, CO*

Mark Orsi, *K12 SIX*

Kent Landfield, *McAfee*

Ginny Badanes, *Microsoft*

Kaja Ciglic, *Microsoft*

Ping Look, *Microsoft*

Jennifer Coughlin, *Mullen Coughlin LLC*

John Guerriero, *National Governors Association*

Justin Herring, *New York Department of Financial Services (NYDFS)*

Adrian McCabe, *Palo Alto Networks*

RTF Membership

Sam Rubin, *Palo Alto Networks*

Sean Morgan, *Palo Alto Networks*

Bob Rudis, *Rapid7*

Scott King, *Rapid7*

Tod Beardsley, *Rapid7*

Allan Liska, *Recorded Future*

Katie Nickels, *Red Canary*

Adam Flatley, *Redacted*

Davis Hake, *Resilience*

Michael Convertino, *Resilience*

Chris Lynam, *Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)*

Jeff Bonvie, *Royal Canadian Mounted Police's National Cybercrime Coordination Unit (NC3)*

Kevin Gronberg, *SecurityScorecard*

Richard Perlotto, *The Shadowserver Foundation*

Beau Woods, *Stratigos Security*

James Shank, *Team Cymru*

Michael Garcia, *Third Way*

Ciaran Martin, *University of Oxford Blavatnik School of Government*

Eleanor Fairford, *U.K. National Cyber Security Centre (NCSC)*

U.K. National Crime Agency (NCA)

Bridgette Walsh, *U.S. Cybersecurity and Infrastructure Security Agency (CISA)*

U.S. Federal Bureau of Investigation (FBI)

Jonah Hill, *U.S. Secret Service (USSS)*

Bobby Chesney, *U.T. Austin Strauss Center*

Who We Are

The Institute for Security and Technology designs and advances solutions to the world's toughest emerging security threats. As a 501(c)(3) non-profit network based in the San Francisco Bay Area, we are dedicated to advancing solutions to critical national security challenges. Our goal is to provide the tools and insights needed for companies and governments to outpace emerging global security threats, creating a bridge between technology and policy leaders.

IST Institute for SECURITY + TECHNOLOGY

Appendix A:
Cyber Insurance

Given the insurance sector's historical role in assessing, managing, pricing, and carrying risks, the cyber insurance industry has been a regular topic of discussion across all of the working groups of the Ransomware Task Force.

This section provides an overview of the cyber insurance market and the role it plays in dealing with ransomware attacks.

Introduction to the Cyber Insurance Market

Many organizations choose to transfer some of their ransomware risk by purchasing insurance. While there are various types of insurance available that may cover losses associated with ransomware, including property insurance, kidnap and ransom insurance, and errors and omissions insurance, most insured ransomware losses are covered by "affirmative" or "stand-alone" cyber insurance. "Affirmative" refers to explicit cyber coverage within the text of an insurance policy; "stand-alone" refers to a dedicated insurance policy for cyber risk, instead of cyber coverage available within a policy dedicated to other types of risk.

The first cyber insurance policies were designed to respond to lawsuits arising out of technology errors and omissions. As the internet developed, organizations digitized their operations, and as states passed laws related to data breach notification and consumer privacy, cyber insurance firms expanded their coverage to respond to the associated risks of data breach and business interruption. Today, cyber insurance has become a standard part of cyber risk management strategies. Many cyber insurers and brokers offer risk management services, education, and security tools to make their insureds more secure, in addition to the traditional risk transfer of an insurance policy.

While many insurance companies actively underwrite cyber risks, the market is led by 20 or so large insurers that write the majority of cyber insurance policies. Less than 15% of organizations globally buy cyber insurance, including about a third of all large companies in the United States. Internationally, the number of companies that have cyber insurance tends to be lower. While cyber insurance is growing, it remains a niche product, and is less than 1% of the size of the greater property and casualty insurance market.[74]

Cyber insurance policies typically cover legal, forensic, and technical experts to help ransomware victims take the most effective steps to recover. (See Table 1, Common Components of a Modern Cyber Insurance Policy.) Insurance concentrates this kind of expertise to help victims best orchestrate their options for recovery. Policies may indemnify victims for any business interruption losses and defend them against any liability arising out of the event. Cyber insurance policies typically cover expertise to help a victim restore

its computer systems from backups and, in the unfortunate circumstances in which the victim has decided it is necessary, expertise to handle a ransom negotiation and effectuate an extortion payment. Cyber insurance policies never require a victim to pay a ransom. Any decision to pay sits with the victim.

TABLE 1: Common Components of a Modern Cyber Insurance Policy

TYPE OF COVERAGE	PARTY	DETAIL
Incident Response Costs	First	The cost of responding to a data breach event, including IT forensics, external services, and specialists that might be employed; internal response costs; legal costs; and costs related to restoring systems to their preexisting condition.
Data Privacy Liability	Third	The cost of dealing with and compensating third-party individuals whose information is or may have been compromised by a data breach event, including notification, compensation, providing credit-watch services, and other third-party liabilities to affected data subjects.
Data Recovery Costs	First	The cost of reconstituting data and/or software that have been deleted or corrupted.
Business Interruption Loss	First	Lost profits or extra expenses incurred due to the unavailability of IT systems or data as a result of cyber attacks or non-malicious IT failures.
Regulatory Defense	Third	Provides coverage for fines, penalties, and defense costs in the face of regulatory actions investigating violations of privacy law.
Cyber Extortion	First	The cost of extortion response expertise to vet and evaluate all possible options for recovery, and, if required, negotiate and execute any ransom payment.
Multimedia Liability	Third	Defense costs and civil damages arising from defamation, libel, slander, copyright/trademark infringement, negligence in publication of any content in electronic or print media, as well as infringement of the intellectual property of a third party.
Reputational Damage	First	Loss of revenues arising from an increase in customer churn or reduced transaction volumes that can be directly attributed to the publication of a defined security breach event.
Network Liability	Third	Third-party liabilities arising from security events occurring within the organization's IT network or passing through it in order to attack a third party.
Contingent Business Interruption Loss	First	Costs of business interruption to the insured resulting from the IT failure of a third party, such as a supplier, critical vendor, utility, or external IT services provider.
Technology Errors & Omissions Liability	Third	Coverage for third-party claims relating to failure to provide adequate technical service or technical products and software, including legal costs and expenses of allegations resulting from a cyber attack, error, or IT failure.
Financial Theft and Fraud	First	The direct financial loss suffered by an organization arising from the use of computers to commit fraud or theft of money, securities, or other property.
Physical Asset Damage	First	First-party loss due to the destruction of hardware or other physical property resulting from cyber attacks.

Thousands of organizations have used cyber insurance to recover from ransomware attacks, including hospitals, cities, and schools, through comprehensive coverage and bringing to bear heavily vetted ransomware response expertise. Each year, cyber insurers pay out hundreds of millions of dollars in cyber losses claimed by their insureds, including business income losses, data recovery costs, and expert fees arising out of ransomware events.[75] As ransomware has become more frequent and destructive, ransomware losses have increased, impacting both insured and insurer. As a result, a number of insurers have exited the cyber insurance market or reduced their participation. Firms that remain have invested heavily in their ability to properly assess cyber risk. With approximately $1 trillion in insurance limits exposed, the cyber insurance market is incentivized to reduce the risks posed by ransomware.

In the insurance industry, periods of falling premiums, expanding coverage, and loosening underwriting standards (resulting from increased competition) are referred to as "soft markets," whereas periods of rising premiums, coverage restrictions, and heightened underwriting standards (due to increased underwriting losses) are often referred to as "hard markets." According to multiple reports, cyber insurance has entered a "hard market" phase.[76]

In a hard market, the insurance industry can push insured organizations to better manage their risk. Competing insurers may do this through rising underwriting standards and risk management strategies, changes to price, and other innovations that align the insured organization's incentives toward risk management and risk transfer. This trend has been seen with respect to perils as diverse as fire, piracy, hurricane, and kidnap for ransom; in each instance, the insurance sector has identified and supported risk management practices and technologies that have bent the curve and ameliorated a significant risk, to the mutual benefit of the insured and the insurer. The cyber insurance market should behave similarly; for example, after the major retail payment card breaches of 2013 and 2014, the cyber insurance market pushed compliance with PCI-DSS standards, industry standards promulgated by the payment card industry that establish a base level of payment card cybersecurity.

In a hard market, the insurance industry can push insured organizations to better manage their risk.

Rising Underwriting Standards in Response to Ransomware

The economics of the cyber insurance industry align with the victims of ransomware. As a result, the industry is incentivized to innovate, evolve, compete, and otherwise increase its expertise to prevent insured ransomware losses. As ransomware losses have accelerated, the cyber insurance market has adapted.

Improved cyber-defense:
The key adaptation has been investment in underwriting analysis to identify ransomware risk factors and developing the expertise to help firms secure themselves appropriately against a ransomware attack. Increased scrutiny of prospective insurance buyers is designed to incentivize firms to make appropriate security investments and become prepared. To accurately measure a firm's ransomware risk, cyber insurers are increasingly deploying supplemental ransomware underwriting applications, enlisting third-party cybersecurity firms to conduct additional assessments, and carrying out external scans of firms' web-facing assets. Cyber insurers may deploy in-house security and risk engineering expertise to proactively help insured organizations become more resilient in the face of ransomware risk. A number of cyber insurers and insurance brokerage firms have established or acquired cybersecurity firms to provide managed threat detection, incident response, or security consulting services to insureds in advance of a loss.

Market Strategies:
Another adaptation comes from cyber insurers experimenting with different market strategies to incentivize organizations to increase their cybersecurity to become secure. These strategies include sublimits (i.e. reduced claim limits) for ransomware-related coverage; co-insurance (the joint assumption of a risk by the insured and insurer); increases in premium; and other changes or requirements in the insurance coverage.[77] Underwriters may refuse to offer insurance coverage to organizations that do not first establish an appropriate level of cybersecurity preparedness. For instance, this may mean that an organization must confirm that it follows a recognized cybersecurity framework, or that it has deployed multi-factor authentication, or is managing the risks associated with remote access to computer networks. While underwriting firms may defer in certain details, the cyber insurance market is coalescing around certain baseline controls as a prerequisite to insurability.[78] Brokerages and risk management firms have also increased their advisory practices to move organizations toward greater ransomware preparedness and insurability.

Organizations that lack basic cybersecurity hygiene may be uninsurable, which should spur greater investment in ransomware defenses. When the market works properly, organizations should be incentivized to reach an appropriate mix of insurance and security.[79]

Process changes:
Finally, as a third adaptation, cyber insurance companies have modified many internal processes. For example, some insurers have established close connections with national and global law enforcement to facilitate the sharing of data and threat intelligence.[80]

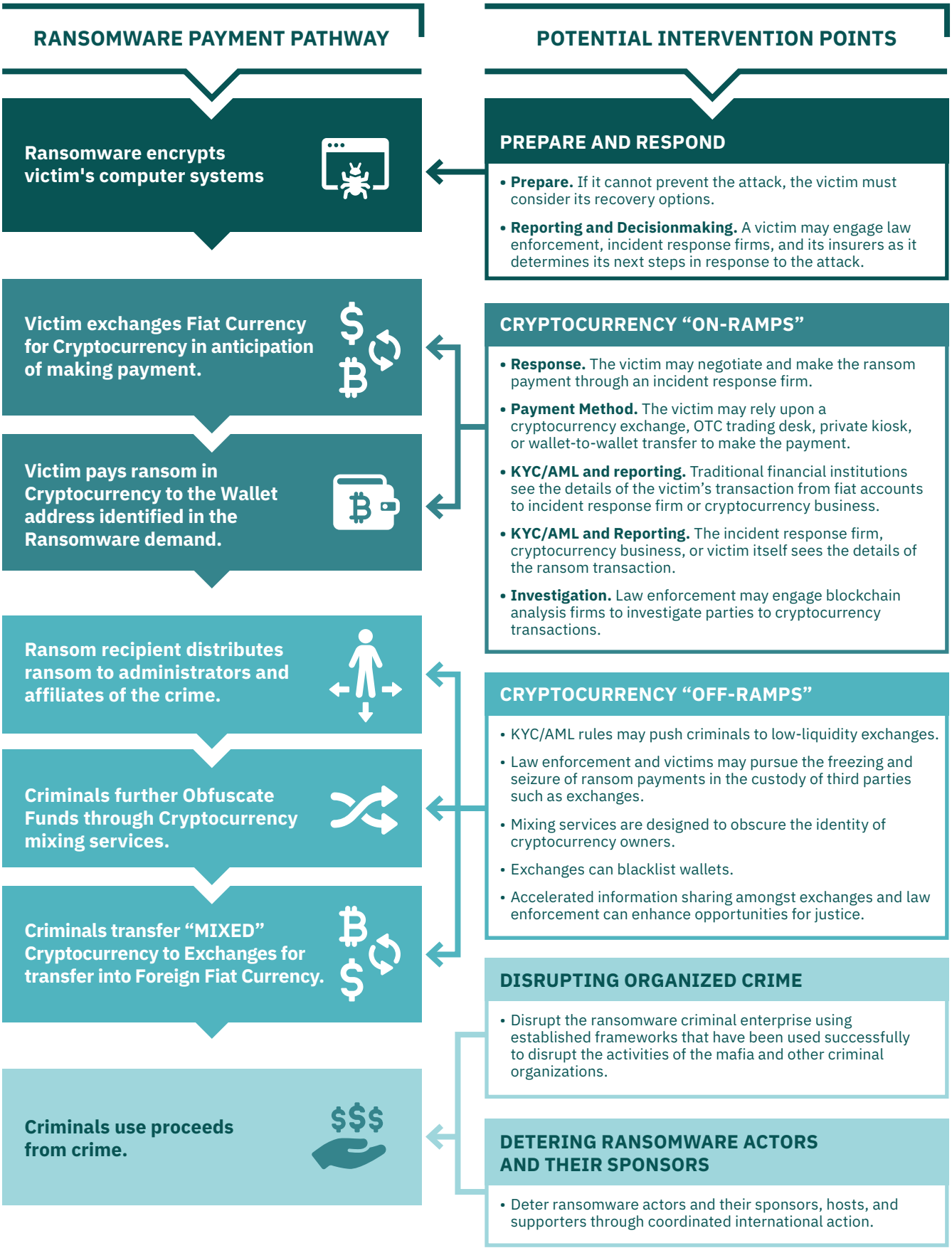
Appendix B:
The Cryptocurrency Payment Process

Ransomware payments are typically made in cryptocurrency. As cryptocurrency ownership records are maintained on the cryptographic ledger of a blockchain, ownership is not easily linked to identifiable individuals. Often the money does not flow straight from victim to criminal; it travels through a multi-step process involving different financial entities, each presenting insights into criminal identities and opportunities for intervention.

This section expounds on this process, identifies many of the key entities involved, and highlights where interventions could occur and how they could undermine the ransomware business model.

The following is a graphical representation of the cryptocurrency payments process, and various potential points of intervention:

Figure 6 Payment Pathway and Potential Intervention Points



1

Step 1 Victim Response

When a victim is hit with a ransomware attack, they may engage one or more incident response entities to assist in the process of advising on, and potentially paying, the ransom. These firms include the victim's cyber-insurance provider (if they have coverage), law firms, negotiation firms, threat intelligence, and forensic investigators.

Entities like negotiation firms communicate directly with ransomware threat actors and seek to lower the ransom demand. Other organizations (for example, incident response firms, financial institutions, etc.) may perform due diligence to ensure a payment would not violate sanctions, identify the extent of applicable insurance coverage, and confirm that there is no publicly available decryption key. These firms may also assist the victim with deciding whether or not to pay the ransom.

2

Step 2 Ransom Payment

If a victim decides to pay the ransom, either they or an incident response vendor, such as a forensic investigator or negotiation firm, will need to withdraw funds from a financial institution to purchase the cryptocurrency. This cryptocurrency is then transferred from the victim's cryptocurrency wallet, a digital storage service, facilitated by a cryptocurrency exchange, a private kiosk, or simply a wallet-to-wallet transfer to a new wallet address provided by the ransomware criminal. These victim-specific addresses are created by the criminal actors for the purpose of receiving the payments. Often these will have never been used before, to avoid being associated with the threat actor's previous activity, and thus cannot be traced until funds are actually deposited into those wallet addresses by the victim. These are generally un-hosted wallets, which means they are not hosted with any cryptocurrency exchange that handles and monitors transactions.

Cryptocurrencies are outside of any one organization's control, but their blockchains create public, permanent records of activity, whether legal or illicit. Blockchain analysis helps interpret public blockchain ledgers and, with the proper tools, government agencies, cryptocurrency businesses, and financial institutions can understand which real-world entities transact with each other. Blockchain analytic companies, such as Chainalysis and CipherTrace, are able to show that a given transaction took place between two different cryptocurrency exchanges, or between a cryptocurrency exchange and an illicit entity, such as a sanctioned individual or organization. With blockchain analysis tools and Know Your Customer (KYC) information, law enforcement can gain transparency into blockchain activity.

While some illicit actors use privacy coins in an attempt to obfuscate their transactions, this more untraceable form of cryptocurrency has not been adopted as widely as might be expected because they are not as liquid as Bitcoin and other cryptocurrencies. Now that many exchanges have delisted privacy coins following guidance from regulators, this payment method is becoming increasingly impractical. Cryptocurrency is only useful if you can buy and sell goods and services or cash out into fiat, and that is much more difficult with privacy coins.

3

Step 3 Ransomware Fund Obfuscation

After receiving the ransomware payment in the designated digital wallet, the ransomware criminal often attempts to obfuscate these funds as quickly as possible to avoid detection and tracking. As noted above, Bitcoin transactions are logged in a public ledger, so without obfuscation, a criminal cannot withdraw funds into cash without being tracked. One popular method for obfuscation is to route funds through cryptocurrency mixing services, services that create a series of transactions to mix one set of funds with another, muddying the public ledger by mixing in legitimate "traffic" with illicit ransomware funds.

Cryptocurrency mixing services

Cryptocurrency mixing services (often "mixers" or "tumblers") are commonly used by ransomware actors and others engaged in illicit activity. As described above, a blockchain is a record of the source and destination of every transaction. As a result, blockchain analytic firms can trace cryptocurrency transactions, supporting both law enforcement efforts to identify criminals and cryptocurrency exchange efforts to screen clients for links to crime. Ransomware actors use mixers to try to prevent such tracing by making it difficult to identify the true source of transactions on the blockchain.

Mixers can function in multiple ways, but typically they rely upon a group of people coming together to pool their cryptocurrency (like bitcoin), with each taking back different bitcoins of the same value. These different bitcoins they receive will have a different source than the ones they submitted for "mixing." This process is typically managed by a centralized mixing service, which charges a fee — often between 1-10% of the amount mixed. Some mixing services take additional steps to complicate and obfuscate the source of funds, including intermediate trades with privacy coins such as Monero. There are hundreds of mixing services available on the internet.

Another method for obfuscation is "chainhopping," exchanging funds in one cryptocurrency for another. Tracking funds after they switch currencies can be extremely challenging. These transactions can occur at centralized or decentralized cryptocurrency exchanges, which are discussed further in Step 4, or via atomic swaps and other technical means.

4

Step 4 Cash out

After obfuscating the funds, ransomware criminals may make use of the cryptocurrency, or withdraw the funds into cash. There are several methods for cashing out, including over-the -counter trading desks, crypto kiosks, and exchanges, which are the most prominent. Others include exchanging bitcoin for gift/debit cards and or alternative coins, such as privacy coins.

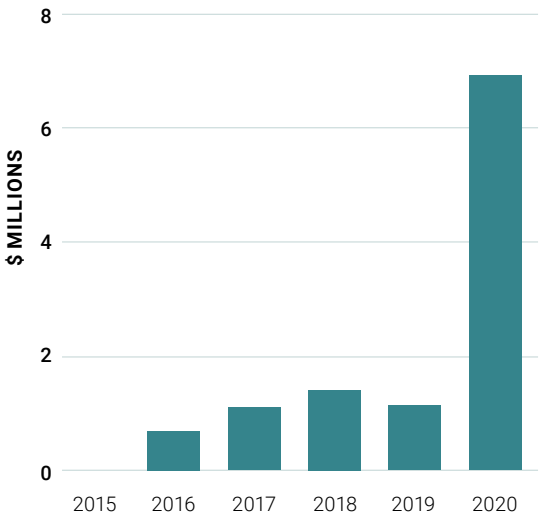
As noted below criminals may make use of cryptocurrency funds by paying for infrastructure to conduct attacks or to pay individuals involved in the criminal organization, such as money launderers and affiliates. Criminals also rely on OTC traders to convert the virtual currency to fiat. A market exists for these OTC transactions because Russian businesses operating in China prefer to operate in Bitcoin to avoid taxes, while criminals operating in Russia prefer cash. Therefore, an OTC trader can connect these individuals with Russian businesses accepting Bitcoin and criminals receiving cash transactions inside Russia.

Where do the funds go?

Ransomware criminals may choose to not immediately withdraw funds into cash for their own use. In the ransomware-as-a-service (RaaS) model described earlier in the report, several criminal affiliates (essentially contractors) are involved in the exploitation, encryption, and ransom demand, all of whom require payouts. Criminal gangs also may use cryptocurrency itself to invest in further malicious infrastructure and services.

In 2020, cryptocurrency-tracing company Chainalysis tracked nearly $7 million sent from ransomware-tainted cryptocurrency wallets to other known illicit marketplaces.[81] Ransoms paid by victims may go on to fund other criminal enterprises that are facilitated online, as has been detailed in other sections of this report.

Figure 7 Ransomware Wallets Sending to Darknet Marketplaces



Step 4 cont...

Cryptocurrency businesses facilitate the trading of cryptocurrency between buyers and sellers. Ransomware criminals rely on these businesses to exchange their ransomware proceeds for different cryptocurrencies or for government-issued currencies. As relatively new financial institutions, these cryptocurrency businesses exist on a spectrum of legitimacy, regulation, and compliance, and handle varying amounts of transactions with illicit funds. For example, in 2019, Coinbase published a report identifying that most exchanges are not in compliance with Anti Money Laundering or Know your Customer procedures.

Cryptocurrency businesses generally fall into one of three categories:

- **Regulated Cryptocurrency Exchanges:** These are legitimate exchanges with high liquidity that are able to handle a large number of transactions. In the United States, these exchanges are subject to non-bank financial institution anti-money laundering (AML) regulations, which require some Know Your Customer (KYC) identification of customers performing large transactions, among other requirements. Other jurisdictions impose similar KYC and AML requirements as those in the United States, including the United Kingdom, the European Union, Japan, Australia and New Zealand.[82]

- **Minimally Regulated Cryptocurrency Exchanges:** Located in jurisdictions with less stringent regulatory obligations than the United States and other members of the G7, these cryptocurrency exchanges operate with few controls for identifying potential illicit funds. These exchanges often serve as one of the preferred services for ransomware criminals to cash out illicit funds without oversight. These exchanges include Binance and Huobi, which have much less stringent KYC rules, especially when dealing with OTC traders.

- **Peer-to-Peer (P2P) Cryptocurrency Exchanges** (also known as Over-the-Counter or Decentralized Exchanges)**:** Regardless of geographical limits, users can download freely-available software or access P2P exchanges to buy and sell cryptocurrency directly with one another. This avoids the use of a third-party service like a "traditional" exchange, which may hold user funds in custody, process transactions in fiat currency, and comply with KYC and AML requirements.

- **Over-The-Counter Trading Desks:** Some OTC traders, actors that trade cryptocurrency without an exchange acting as a facilitator or mediator of the trade, provide cryptocurrency laundering services to ransomware threat actors. Although many OTC traders maintain legitimate businesses and comply with stringent financial regulations, some do not, and they provide an important source of liquidity for exchanging ransomware payment.

Tracking payments is difficult due to the variance in standards and enforcement of regulation for exchanges of different categories, or that operate in different countries. Even using regulated exchanges, ransomware actors constantly find new ways to remain hidden by using money mule service providers to set up accounts, or use accounts with false or stolen credentials.

Appendix C:
Proposed Framework for a Public-Private Operational Ransomware Campaign

This appendix provides an overview of how the formal, government-led Joint Ransomware Task Force (JRTF) and the informal Ransomware Threat Focus Hub (RTFH) could collaborate to conduct an operational ransomware campaign.

Background

Over the years, many efforts have attempted to formalize the trust networks that are relied on to keep the internet operating. Some initiatives have been effective without significant formal structure: the Conficker Working Group, convened by Microsoft in the late 2000s to stop the spread and impact of the Conficker worm, is often lauded as an early model. More formal joint collaborative efforts have also been successful: the 2020-2021 takedown of Emotet was an example of a long collaborative effort between global law enforcement, judicial authorities, and private industry to seize and disrupt a massive global botnet. More often, though, public-private information security collaboration occurs primarily when there is a crisis, as was the case with the Cyber Unified Coordination Group (UCG), which the U.S. Government convened in 2021 to focus on the Hafnium case involving vulnerable Microsoft Exchange Servers.

What remains elusive is a standing mechanism for convening operationally focused, sustained, public-private campaigns that are coordinated via formal and informal nodes, and that allow for both the formal requirements needed by government and the informal requirements needed by industry. Much has already been written about potential solutions for launching such an initiative, including Jay Healey's 2018 article on Cyber Incident Collaboration Organizations,[83] recent work by the Aspen Institute,[84] and recommended solutions from the World Economic Forum's Partnership Against Cybercrime.[85] Ransomware presents a unique opportunity to test new approaches, and the Ransomware Task Force provides below a proposed framework for consideration.

Objective

Use operational collaboration to increase the scope, scale, pace, and efficacy of intelligence-driven takedowns and disruption of ransomware operations and the infrastructure and people that enable them.

Assumptions

Ransomware actors are intelligently taking advantage of the seams between law enforcement and private-sector cooperation mechanisms, and between governmental and private-sector legal authorities. They also move with such alacrity that existing structures cannot respond fast enough to disrupt their activities on a sustained, rapid, and concerted basis.

Existing mechanisms are working to address the problem, but they are siloed in various agencies and not leveraging the full authorities and capabilities of all government agencies. They also do not routinely incorporate private-sector action, nor do they scale to compete with the agility of the criminals.

This public-private operational collaboration mechanism should include actors and organizations that are involved in the full gamut of defending against and disrupting ransomware operations. No single actor or entity is fully capable of disrupting this threat by itself, so public and private actors must come together to assess the threat and coordinate activities across authorities and capabilities.

Private-sector participants must recognize that not all government actions will be shared or coordinated with non-government actors due to security concerns or to protect sources and methods.

Government participants must recognize that private-sector participants may need to take actions quickly to protect their customers and fulfill contractual agreements, and may not always be able to coordinate actions with the government.

A natural governmental response to this collaboration requirement is to create some kind of formal structure. However, a formal private-public Joint Ransomware Task Force would likely hinder private-sector participation. Past experience has shown that private-sector participants are more likely to share information with the government and take actions to defend their customers in coordination with government through existing informal and indirect channels. The U.S. Government, on the other hand, needs formality to function in a joint way; moreover, the need for public accountability requires the government to adhere to formal rules and structures. Departments and agencies, especially those with competing equities, are more likely to work only within their lane of authorities and capabilities unless they are required and incentivized to work with each other.

Thus a formal government task force paired with existing formal and informal private-sector groups in the short-term would build trust and work to develop some early wins. Over time, a combination of formal and informal private-sector structures should develop to interface with the government's Joint Ransomware Task Force (JRTF), working toward a 24/7 operational collaboration mechanism for a public-private anti-ransomware campaign.

Ransomware disruptions will almost always be law enforcement operations at their core. But in order to truly disrupt ransomware actors, we must also consider non-law enforcement options and capabilities that can improve defenses, impose costs, or more fully disrupt ransomware operations. In terms of the intelligence needed for such operations, the government and various private-sector organizations need each other.

*Over time, a combination of formal and informal private sector structures should develop to interface with the government's Joint Ransomware Task Force, working towards a **24/7** operational collaboration mechanism for a public-private anti-ransomware campaign.*

- Private-sector cybersecurity providers are often best positioned to capture indicators of compromise and tactics, techniques, and procedures (TTPs) of the malicious actors to develop protections for their customers and understand active campaigns.
- Cryptocurrency exchanges and analysis firms are best positioned to understand the flow of ransomware payments.
- Government agencies, especially in law enforcement and the Intelligence Community, are best positioned to identify the individuals behind the activity.
- All of these intelligence perspectives must be shared, combined, and understood in order to develop the best possible disruption options.

U.S. Government personnel working with the private sector in a given campaign must be empowered and incentivized by their leadership to engage with the private sector and take action based on what they learn. They should also anticipate the needs of private-sector partners and share information that will lead to disruptions.

To achieve this increased level of operational collaboration, the Ransomware Task Force recommends the following:

Recommendations

1. The U.S. Government should establish the Joint Ransomware Task Force (JRTF) consisting of representatives from the Cybersecurity and Infrastructure Security Agency (CISA; the FBI; United States Secret Service; the Intelligence Community; U.S. Cyber Command; the Departments of Treasury, Justice, and State; the Office of the National Cyber Director; and other departments and agencies as appropriate. The JRTF's mission should be to prioritize ransomware disruption operations and leverage the intelligence-driven disruption planning process to increase the pace and efficacy of ransomware takedowns and disruption. The Departments of Homeland Security, Justice, and Defense should jointly provide the resources needed to establish and operate the Task Force, such as office space, IT infrastructure, and other supplies. The Task Force should coordinate closely with the Joint Cyber Planning Office in CISA, the National Cyber Investigative Joint Task Force (NCIJTF), and other inter-agency cyber-related groups. The NSC-led Interagency Working Group recommended in 1.2.1 of the main RTF report would provide direction, priorities, and oversee the JRTF. The goals of the JRTF should be to:

    - Prioritize intelligence-driven operations to disrupt specific ransomware actors;
    - Incentivize and empower government agencies and personnel to participate in joint operations in the interagency and with private-sector partners and take action; and
    - Anticipate the needs and requests of the private sector

    The Administration could create such a Task Force through executive action, just as the Bush Administration created the NCIJTF through National Security Policy Directive-54/Homeland Security Policy Directive-23. The JRTF could be a stand-alone entity, or as U.S. government cyber organizations continue to mature and evolve, it could be folded into an existing organization, such as the Joint Cyber Planning Office, the National Cyber Director's office, or the NCIJTF.

2. An existing non-profit organization should establish a private-sector Ransomware Threat Focus Hub. The participants should include cybersecurity providers, non-profit sharing organizations, cyber threat intelligence firms, threat intelligence researchers and contractors, incident response firms, managed security service providers, telecommunications companies, major platform owners/operators, and hosting providers. The Hub would facilitate and coordinate sustained private-sector actions against an agreed-upon target list, in coordination with the JRTF. The hosting non-profit organization, such as an information-sharing and analysis organization (ISAO), would provide space for information sharing and operational collaboration between participants.[86] Formal and informal coordination could occur within this Hub, and the Hub would encourage informal and formal groups to work together in tandem. Informal groups would continue to work and collaborate as they do today, while the formal layer would focus on long-term, permanent arrangements with the U.S. or other governments.

The RTF recommends the following general tasks for the JRTF and the RTFH:

Proposed JRTF Tasks

1. Establish a "target list" of the top 10 ransomware threats, in consultation with the private-sector hub, updated on an ongoing basis, to:
   a. Identify and prioritize targets for threat cells, focused on specific ransomware actors/conglomerates;
   b. Identify a timeline for the operation; and
   c. Identify metrics for success.
2. Disrupt criminal actors, associated infrastructure, and their finances.
3. Enable private-sector representatives to move against ransomware actors and infrastructure with rapid legal authority (e.g. court orders) when necessary to take required actions.
4. Enable the private sector to tip and cue law enforcement, network defenders, intelligence community, and, where necessary, U.S. military action.
5. Collect, share, and analyze ransomware trends to inform campaigns.
6. Create "after action reports" that identify successes and failures in an operation to improve subsequent operations.
7. Use non-traditional tools, such as information and influence operations, through online forums or a dedicated web portal

Proposed Ransomware Threat Focus Hub Tasks:

1. Provide input to the JRTF's top 10 target list.
2. Take synchronized actions against criminal actors, associated infrastructure, and financial operations, based on participants' legal authority.
3. Enable government-sector representatives to target and disrupt ransomware actors and infrastructure more rapidly.
4. Collect, share, and analyze ransomware trends to inform counter-ransomware campaigns.
5. Create "after action reports" from the private-sector point of view that identify successes and failures in each operation to improve subsequent operations.
6. Use non-traditional tools, such as information and influence operations, via online forums, a dedicated web portal, or other means.

Glossary

AG	Attorney General
ALATs	Assistant Legal Attachés
APAC	Asia-Pacific
Atomic Swaps	A smart contract technique that allows the quick exchange of two different cryptocurrencies, running on distinct blockchain networks, without using centralized intermediaries.
AML	Anti-Money Laundering
CCIPS	Computer Crime and Intellectual Property Section
CDNs	Content Delivery Networks
Centralized Cryptocurrency Exchange (CEX)	Online platforms that are used to buy and sell cryptocurrencies. They are the most common means that investors use to buy and sell cryptocurrency holdings. Most of the control over your account remains in the hands of the third party that runs the exchange
CFAA	Computer Fraud and Abuse Act
CFT	Combatting Financing of Terrorism
CHIPS	Computer Hacking and Intellectual Property Network
CISA	Cybersecurity and Infrastructure Security Agency
CNO	Computer Network Operations
CRRFs	Cyber Response and Recovery Funds
CSN	Cybercrime Support Network
Cyber Kill Chain	A series of steps that trace the stages of a cyberattack from the early reconnaissance stages to the exfiltration of data. The steps are as follows: 1. ***Reconnaissance:*** The observation stage: attackers typically assess the situation from the outside in to identify both targets and tactics for the attack. 2. ***Intrusion:*** Based on what the attackers discovered in the reconnaissance phase, they are able to get into the systems: often leveraging malware or security vulnerabilities. 3. ***Exploitation:*** The act of exploiting vulnerabilities, and delivering malicious code onto the system. 4. ***Privilege Escalation:*** Attackers often need more privileges on a system to get access to more data and permissions. For this, they need to escalate their privileges, often to an Admin.

5. ***Lateral Movement:*** Once in the system, attackers can move laterally to other systems and accounts in order to gain more leverage, whether higher permissions, more data, or greater access to systems.
6. ***Obfuscation / Anti-forensics:*** In order to successfully pull off a cyberattack, attackers need to cover their tracks; during this stage, they often lay false trails, compromise data, and clear logs to confuse and/or slow down any forensics team.
7. ***Denial of Service:*** Disruption of normal access for users and systems, in order to stop the attack from being monitored, tracked, or blocked.
8. ***Exfiltration:*** The extraction stage: getting data out of the compromised system.

Decentralized Cryptocurrency Exchange (DEX)	A peer-to-peer (P2P) marketplace that connects cryptocurrency buyers and sellers. A user remains in control of their private keys when transacting on a DEX platform.
DFIR	Digital Forensics/Incident Response
DHS	Department of Homeland Security
DNS	Denial of Service
DSAR	Data Subjection Access Request
EMEA	Europe, the Middle East, and Africa
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
Fiat	Government-issued currency that is not backed by a commodity such as gold; often has government regulations.
FinCEN	Financial Crimes Enforcement Network
FSB	Federal Security Service
HAVA	Help America Vote Act
HIPAA	Health Insurance Portability and Accountability Act
HITECH ACT	Health Information Technology for Economic and Clinical Health Act
HSMs	Hardware Security Models
HUMINT	Human Intelligence
ICA	Intelligence Community Assessment
ICHIP	International Computer Hacking and Intellectual Property
IMINT	Imagery Intelligence
IOS	Indicators of Compromise
IRS	Internal Revenue Service
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization

IWG	Interagency Working Group
JCPO	Joint Cyber Planning Office
JRTF	Joint Ransomware Task Force
KYC	Know Your Customer
Know Your Customer (KYC) Information	A standard in the investment industry that ensures investment advisors know detailed information about their clients' risk tolerance, investment knowledge, and financial position. Sharing KYC information on blockchain would enable financial institutions to deliver better compliance outcomes, increase efficiency, and improve customer experience. Information includes name, date of birth, address, bills, etc.
MDBR	Malicious Domain Blocking and Reporting
Money Mule Service Providers	Someone who transfers or moves illegally acquired money on behalf of someone else. Criminals recruit money mules to help launder proceeds derived from online scams and frauds or crimes.
MS-ISAC	Multi-State Information Sharing and Analysis Center
MSB	Money Service Businesses
MSP	Managed Service Providers
MSSP	Managed Security Services Providers
MXs	Mail Exchangers
NAIC	National Association of Insurance Commissioners
NCD	National Cyber Director
NCIJTF	National Cyber Investigative Joint Task Force
NCSC	National Cyber Security Centre
NDAA	National Defense Authorization Act
NIS Directive	Network and Information Security Directive
NIST	National Institute of Standards and Technology
NSC	National Security Council
NSD	National Security Division
OFAC	Office of Foreign Assets Controls
OFE	Office of Fraud Enforcement
OTC	Over the counter
PCI DSS	Payment Card Industry Data Security Standard
Privacy Coins	A class of cryptocurrencies that power private and anonymous blockchain transactions by obscuring their origin and destination.
RAAS	Ransomware as a Service, a business model used by ransomware developers, in which they lease ransomware variants in the same way that legitimate software developers lease software as a service (SaaS) products.

RCE	Remote Code Execution
RICO	Racketeer Influenced and Corrupt Organizations Act
RIR	Ransomware Incident Report (proposed)
RIRN	Ransomware Incident Response Network (proposed)
RTF	Ransomware Task Force
RTFH	Ransomware Threat Focus Hub (proposed)
SARs	Suspicious Activity Reports
SDN List	Specially Designated Nationals and Blocked Person List
SEC	U.S. Securities and Exchange Commission
SIGINT	Signals Intelligence
SLTTs	U.S. State, local, tribal, and territorial government entities
Trust Group	Communities of security professionals who collaborate between chains of trust. Trust Groups' missions often include maintaining integrity and security of the internet, developing and sharing information, and encouraging and promoting security.
TS/SCI	Top Secret / Sensitive Compartmented Information
TTP	Tactics, Techniques, and Procedures
UCG	Cyber Unified Coordination Group
USAOs	United States Attorney's Office
USIC	United States Intelligence Community

Endnotes

1. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emisoft Blog, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

2. Coveware, "Ransomware Payments Fall as Fewer Companies Pay Data Exfiltration Extortion Demands," February 1, 2021. https://www.coveware.com/blog/ransomware-marketplace-report-q4-2020

3. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emisoft Blog, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

4. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," excerpt from the Chainalysis 2021 Crypto Crime Report, January 26, 2021, https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

5. Unit 42, Palo Alto Networks, "Ransomware Threat Assessments: A Companion to the 2021 Unit 42 Ransomware Threat Report," March 17, 2021, https://unit42.paloaltonetworks.com/ransomware-threat-assessments.

6. Commandant, U.S. Coast Guard, "Marine Safety Information Bulletin: Cyberattack Impacts MTSA Facility Operations," December 2019. https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf

7. Rundle, James and Nash, Kim S. "Ransomware Attack Exposes Poor Energy-Sector Cybersecurity," Wall Street Journal, February 2020, https://www.wsj.com/articles/ransomware-attack-exposes-poor-energy-sector-cybersecurity-11582540200.

8. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emisoft Blog, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

9. Eddy, Melissa and Perlroth, Nicole. "Cyber Attack Suspected in German Woman's Death," New York Times, September 18, 2020. https://www.nytimes.com/2020/09/18/world/europe/cyber-attack-germany-ransomeware-death.html.

10. Barry, Ellen and Perlroth, Nicole. "Patients of a Vermont Hospital Are Left 'in the Dark' After a Cyberattack," November 26, 2020. https://www.nytimes.com/2020/11/26/us/hospital-cyber-attack.html.

11. Krebs, Brian. "Study: Ransomware, Data Breaches at Hospitals tied to Uptick in Fatal Heart Attacks," KrebsOnSecurity, November 7, 2019, https://krebsonsecurity.com/2019/11/study-ransomware-data-breaches-at-hospitals-tied-to-uptick-in-fatal-heart-attacks/.

12. Hay Newman, Lily. "Atlanta Spent $2.6M to Recover From a $52,000 Ransomware Scare," Wired. April 23, 2018. https://www.wired.com/story/atlanta-spent-26m-recover-from-ransomware-scare/

13. Coble, Sarah. "MAZE Exfiltration Tactic Widely Adopted," Infosecurity Magazine. Accessed April 2, 2021. https://www.infosecurity-magazine.com/news/maze-exfiltration-tactic-widely/.

14. Emsisoft Malware Lab, "The State of Ransomware in the US: Report and Statistics 2020," January 18, 2021, Emisoft Blog, https://blog.emsisoft.com/en/37314/the-state-of-ransomware-in-the-us-report-and-statistics-2020/

15. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Actors Target K-12 Distance Learning Education to Cause Disruptions and Steal Data," December 10, 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-345a

16. Associated Press. "Baltimore: Ransomware Attack Will Cost at Least $18M," May 30, 2019. https://www.nbcwashington.com/news/local/baltimore-ransomware-attack-will-cost-at-least-18m/159464/

17. Chokshi, Niraj. "Hackers Are Holding Baltimore Hostage: How They Struck and What's Next,"New York Times, May 22, 2019. https://www.nytimes.com/2019/05/22/us/baltimore-ransomware.html

18. Freed, Benjamin. "Baltimore ransomware attack was early attempt at data extortion, new report shows," StateScoop, September 25, 2020. https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/

19. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," January 26, 2021. Exerpt from Chainalysis 2021 Crypto Crime Report. https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

20. Buckley, Eileen. "Ransomware attack shutdown all Buffalo school learning," The Rebound Buffalo, March 15, 2021. https://www.wkbw.com/rebound/state-of-education/ransomware-attack-shutdown-all-buffalo-school-learning

21. Coble, Sarah. "Cyber-Attack on Mississippi Schools Costs $300,000," InfoSecurity Magazine, Accessed on April 10, 2021. https://www.infosecurity-magazine.com/news/cyberattack-on-mississippi-schools/

22. Palmer, Danny. "A highly sophisticated ransomware attack leaves 36,000 students without email," ZDNet, March 30, 2021. https://www.zdnet.com/article/a-highly-sophisticated-ransomware-attack-leaves-36000-students-without-email/

23. Weston, Sabina. "Evidence suggests REvil behind Harris Federation ransomware attack," ITPro, April 9, 2021. https://www.itpro.com/security/ransomware/359161/evidence-suggests-revil-behind-harris-federation-ransomware-attack

24. Cybersecurity & Infrastructure Security Agency (CISA), "Ransomware Guidance and Resources," https://www.cisa.gov/ransomware

25. Sophos, "The State of Ransomware 2020," May 2020. http://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/pdf/sophos-the-state-of-ransomware-2020-wp.pdf

26. United States Department of Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," October 1, 2020. https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf

27. Sentonas, Michael. "2020 Global Security Attitude Survey: How Organizations Fear Cyberattacks Will Impact Their Digital Transformation and Future Growth," CrowdStrike Blog, November 17, 2020. https://www.crowdstrike.com/blog/global-security-attitude-survey-takeaways-2020

28. Cyber Florida, "The Connection Between Ransomware and Cyber Insurance Claims in 2020," October 20, 2020, Cyber Florida, https://cyberflorida.org/best-practices/the-connection-between-ransomware-and-cyber-insurance-claims-in-2020/

29. Dudley, Renee. "The Extortion Economy: How Insurance Companies Are Fueling a Rise in Ransomware Attacks," https://www.propublica.org/article/the-extortion-economy-how-insurance-companies-are-fueling-a-rise-in-ransomware-attacks

30. Smilyanets, Dmitry. "'I scrounged through the trash heaps… now I'm a millionaire:' An interview with REvil's Unknown," The Record. March 16, 2021. https://therecord.media/i-scrounged-through-the-trash-heaps-now-im-a-millionaire-an-interview-with-revils-unknown/

31. Freedman, Linn F. "Sodinokibi Hackers Switch Payment Mechanism to Monero," National Law Review, April 16, 2020. https://www.natlawreview.com/article/sodinokibi-hackers-switch-payment-mechanism-to-monero

32. Reuters, "Cyber attack hits 200,000 in at least 150 countries: Europol," May 14, 2017. https://www.reuters.com/article/us-cyber-attack-europol/cyber-attack-hits-200000-in-at-least-150-countries-europol-idUSKCN18A0FX

33. Sophos, "The State of Ransomware 2020," May 2020. http://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/pdf/sophos-the-state-of-ransomware-2020-wp.pdf

34. Check Point. Live Cyber Threat Map. https://threatmap.checkpoint.com/

35. Khan, Abdullah. "G7 finance ministers urge countries to adopt FATF standards against cybercrime," S&P Global Market Intelligence, Oct.13, 2020. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/g7-finance-ministers-urge-countries-to-adopt-fatf-standards-against-cybercrime-60717238

36. Skulkin, Oleg; Rezvukhin, Roman; Rogachev, Semyon, "Ransomware Uncovered 2020/2021," Group IB, March 2021, https://www.group-ib.com/resources/threat-research/ransomware-2021.html

37. Midler, Marisa. "Ransomware as a Service Threats," Carnegie Mellon Univesrity Software Engineering Institute Blog. October 5, 2020. https://insights.sei.cmu.edu/blog/ransomware-as-a-service-raas-threats/. See also Kost, Edward, "What is Ransomware as a Service (RaaS)? The dangerous threat to world security," UpGuard Blog, March 5, 2021. https://www.upguard.com/blog/what-is-ransomware-as-a-service

38. United States Department of the Treasury, "DPRK Cyber Threat Advisory: Guidance on the North Korean Cyber Threat," April 15, 2020. https://home.treasury.gov/system/files/126/dprk_cyber_threat_advisory_20200415.pdf

39. United States Department of the Treasury, "Treasury Sanctions Russia with Sweeping New Sanctions Authority," Press Release, April 15, 2021. https://home.treasury.gov/news/press-releases/jy0127

40. G7, "Ransomware Annex to G7 Statement," October 13, 2020, https://home.treasury.gov/system/files/136/G7-Ransomware-Annex-10132020_Final.pdf

41. Details about the NotPetya ransomware attack from: Perlroth, Nicole. This is How They Tell Me the World Ends, New York: Bloomsbury Publishing, 2021; and Greenberg, Andy. Sandworm, 2019. New York: Penguin Random House.

42. See, for example, Center for Internet Security, "CIS Controls," https://www.cisecurity.org/controls/.

43. See, for example, National Institute of Standards and Technology (NIST), "Small Business Cybersecurity Corner: Training," https://www.nist.gov/itl/smallbusinesscyber/training

44. Ibid

45. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Incident Response," https://www.cisa.gov/cyber-incident-response

46. Testimony from Donna F. Dodson, Chief Cybersecurity Advisor, National Institute of Standards and Technology, United States Department of Commerce, "Strengthening Public-Private Partnerships to Reduce Cyber Risks to Our Nation's Critical Infrastructure," https://www.nist.gov/speech-testimony/strengthening-public-private-partnerships-reduce-cyber-risks-our-nations-critical

47. Cybersecurity & Infrastructure Security Agency (CISA), "CISA Launches Campaign to Reduce the Risk of Ransomware," Press Release, January 21, 2021. https://www.cisa.gov/news/2021/01/21/cisa-launches-campaign-reduce-risk-ransomware

48. For more about "No More Ransom," see https://www.nomoreransom.org.

49. National Cyber Security Centre (NCSC), "Mitigating malware and ransomware attacks," February 13, 2020. https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

50. Europol, "World's Most Dangerous Malware EMOTET Disrupted Through Global Action," Press Release, January 27, 2021. https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

51. Other potential forums include the Five Eyes LE Group, Five Eyes AG Group, Tech Accord (PS), Global Banking Associations, Electronic Banking Group, European Banking Federation, Organisation for Security and Cooperation in Europe, World Economic Forum, and Ottawa F5 - AU.

52. Five Country Ministerial, "Five Country Ministerial Statement Regarding the Threat of Ransomware," April 7/8, 2021. https://www.beehive.govt.nz/sites/default/files/2021-04/Five%20Country%20Ministerial%20Statement%20Regarding%20the%20Threat%20of%20Ransomware.pdf

53. In October 2020, finance ministers from the Group of Seven called upon nations to implement Financial Action Task Force standards to reduce ransomware and other cyber crime. See Khan, Abdullah. "G7 finance ministers urge countries to adopt FATF standards against cybercrime," S&P Global Market Intelligence, Oct.13, 2020. https://www.spglobal.com/marketintelligence/en/news-insights/latest-news-headlines/g7-finance-ministers-urge-countries-to-adopt-fatf-standards-against-cybercrime-60717238

54. See Europol, "Joint Cybercrime Action Taskforce," https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce.

55. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," excerpt from the Chainalysis 2021 Crypto Crime Report, January 26, 2021, https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

56. The Financial Crimes Enforcement Network (FinCEN) has proposed a rule to tighten compliance around convertible virtual currencies and digital assets. See Department of the Treasury, Financial Crimes Enforcement Network, "Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets," https://public-inspection.federalregister.gov/2020-28437.pdf

57. See U.S. Department of Treasury, "Section 314(b) Fact Sheet," https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf

58. Versprille, Allyson. "IRS's 'Operation Hidden Treasure' Focusing on Crypto Fraud," Bloomberg Tax, March 5, 2021. https://news.bloombergtax.com/daily-tax-report/irss-operation-hidden-treasure-focusing-on-crypto-fraud

59. See the International Organization for Standardization (ISO), https://www.iso.org/publication-list.html

60. National Institute of Standards and Technology (NIST), "Cybersecurity Framework," https://www.nist.gov/cyberframework

61. SecurityScorecard identified 10 security issues more prevalent in ransomware victims than other organizations; if companies addressed these issues they could lower their risk of a successful ransomware attack. See Peng, Tishun Peng and Sohval, Bob. "Organizations with Diligent Cybersecurity Less Likely to Fall Victim to Costly Ransomware," April 15, 2021. https://securityscorecard.com/blog/organizations-with-diligent-cybersecurity-practices-less-likely-to-fall-victim-to-costly-ransomware-attacks

62. See, for example, U.S. Department of Health and Human Services (HHS), "Ransomware Fact Sheet," https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

63. Center for Internet Security, Malicious Domain Blocking and Reporting (MDBR), https://www.cisecurity.org/ms-isac/services/mdbr/

64. Cybersecurity & Infrastructure Security Agency (CISA), "Cyber Hygiene Services," https://www.cisa.gov/cyber-hygiene-services

65. Center for Internet Security, CIS Controls V7.1 Implementation Groups, https://www.cisecurity.org/white-papers/cis-controls-v-7-1-implementation-groups/

66. National Institute of Standards and Technology (NIST), "Cybersecurity Framework," https://www.nist.gov/cyberframework

67. Garcia, Michael. "Follow the Money: Few Federal Grants are Used to Fight Cybercrime," Third Way, February 16, 2021. https://www.thirdway.org/report/follow-the-money-few-federal-grants-are-used-to-fight-cybercrime

68. See "H.R.7898 - To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes," https://www.congress.gov/bill/116th-congress/house-bill/7898/text?r=2&s=1

69. United States Cyberspace Solarium Commission, March 2020. https://drive.google.com/file/d/1ryMCIL_dZ30QyjFqFkkf10MxIXJGT4yv/view

70. U.S. Department of Treasury, "Terrorism Risk Insurance Program," https://home.treasury.gov/policy-issues/financial-markets-financial-institutions-and-fiscal-service/federal-insurance-office/terrorism-risk-insurance-program

71. For more about the Structured Threat Information eXpression (STIX™), see https://stixproject.github.io/.

72. For more on the MITRE ATT&CK® Framework, see https://attack.mitre.org.

73. Congressional bill S. 4226 (116th): Assessing a Cyber State of Distress Act of 2020. https://www.govtrack.us/congress/bills/116/s4226/summary

74. Memorandum from Matthews, Denise, Director, Data Coordination and Statistical Analysis National Association of Insurance Commissioners and the Center for Insurance Policy and Research. "Report on the Cybersecurity Insurance and Identity Theft Coverage Supplement," December 4, 2020. https://content.naic.org/sites/default/files/inline-files/Cyber_Supplement_2019_Report_Final_1.pdf

75. Marsh JLT Specialty, "Setting the Record Straight on Cyber Insurance," https://www.marsh.com/us/insights/research/setting-the-record-straight-on-cyber-insurance.html

76. See, for example, "Aon's E&O | Cyber Insurance Snapshot," https://www.aon.com/cyber-solutions/wp-content/uploads/Aon-errors-and-omissions-cyber-insurance-snapshot.pdf; "Cyber may never experience another soft market: Gallagher Re," Intelligent Insurer, April 14, 2021, https://www.intelligentinsurer.com/news/cyber-may-never-experience-another-soft-market-gallagher-re-25350; 2021 Cyber Insurance Market Conditions Report, https://www.ajg.com/us/news-and-insights/2021/jan/2021-cyber-insurance-market-report.

77. Hewitt Jones, John. "Cyber insurers tighten controls as ransomware pain increases," Inside P&C, September 28, 2020, https://insuranceinsider.com/p-and-c/articles/135862/cyber-insurers-tighten-controls-as-ransomware-pain-increases

78. See, for example, Doernberg, John, "Ransomware Causes Cyber Insurers to Raise the Bar," Gallagher, https://www.ajg.com/us/news-and-insights/2021/apr/cyber-insurance-fight-against-ransomware.

79. Studies addressing how cyber insurance may shape an organization's cybersecurity decision-making include: Romanosky, Sasha, Ablon, Lillian, Kuehn, Andreas, and Jones, Therese. "Content analysis of cyber insurance policies: how do carriers price cyber risk?" Journal of Cybersecurity, February 27, 2019, https://academic.oup.com/cybersecurity/article/5/1/tyz002/5366419; Harrison, Richard and Herr, Trey (editors). "Cyber Insecurity: Navigating the Perils of the Next Information Age," https://www.cyberinsecuritybook.org/; Sullivan, James and Nurse, Jason RC. "Cyber Security Incentives and the Role of Cyber Insurance," Royal United Services Institute for Defence and Security Studies and University of Kent. https://rusi.org/sites/default/files/246_ei_cyber_insurance_final_web_version.pdf

80. See, for example, Stone, Jeff. "FBI turns to insurers to grasp the full reach of ransomware," Cyberscoop, March 30, 2020, https://www.cyberscoop.com/ransomware-fbi-insurance-companies-data/; Lyngaas, Sean. "Inside the FBI's quiet 'ransomware summit," Cyberscoop, November 16, 2019, https://www.cyberscoop.com/fbi-ransomware-summit/

81. Chainalysis Team, "Ransomware Skyrocketed in 2020, But There May Be Fewer Culprits Than You Think," excerpt from the Chainalysis 2021 Crypto Crime Report, January 26, 2021, https://blog.chainalysis.com/reports/ransomware-ecosystem-crypto-crime-2021

82. Protiviti , "Guide to US Anti-Money Laundering Requirements, Frequently Asked Questions, Sixth edition https://www.protiviti.com/sites/default/files/united_states/insights/guide-to-us-aml-requirements-6thedition-protiviti_0.pdf

83. Healey, Jason. "Innovation on cyber collaboration: Leverage at scale," Atlantic Council, May 3, 2018, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/innovation-on-cyber-collaboration-leverage-at-scale/

84. Aspen Cybersecurity Group, "An Operational Collaboration Framework," November 8, 2018, https://www.aspeninstitute.org/publications/an-operational-collaboration-framework/

85. World Economic Forum, "Partnership Against Cybercrime: Insight Report," November 2020, http://www3.weforum.org/docs/WEF_Partnership_against_Cybercrime_report_2020.pdf

86. Cybersecurity & Infrastructure Security Agency (CISA), "Information Sharing and Analysis Organizations," https://www.cisa.gov/information-sharing-and-analysis-organizations-isaos