Ransomware Attacks on Critical Infrastructure Sectors

2022 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

I. Executive Summary

Ransomware is a **national security threat** often compared to terrorism.[i] Like terrorism, ransomware focuses on soft targets like civilian critical infrastructure, but unlike terrorism, it is primarily **financially motivated**. US Government (USG) policy must address the **visibility** of incidents and the **profitability** of ransomware, including victims' incentives to pay ransoms.

Ransomware gangs constantly **attack Critical Infrastructure (CI)**, but many attacks go **unreported,** particularly when no ransom is paid. In 2016[ii] and 2017,[iii] different AEP groups warned that ransomware was likely to grow, and it has grown exponentially since then.[iv,v] Accurate data on the frequency of ransomware attacks on critical infrastructure is essential to plan, execute, and evaluate the effectiveness of USG counter-ransomware efforts. "The federal government lacks comprehensive data on ransomware attacks" and "reporting is fragmented across multiple federal agencies," according to the recent Peters Report.[vi] USG receives reports on ransom payments via the Financial Crimes Enforcement Network (FinCEN) and on ransomware incidents via Cybersecurity and Infrastructure Security Agency (CISA) and law enforcement (LE); we offer recommendations to improve whole-of-government visibility by addressing intelligence sharing and improving the reporting process.

Counter-ransomware efforts must address **incentives** by making it **harder for ransomware gangs to get paid** and by **deterring future attacks**. USG has made significant efforts to target funding: sanctioning cash-out operations (primarily in Central and Eastern Europe) and tightening regulations on cryptocurrency exchanges linked to ransomware domestically and in partner countries like Estonia. However, it is too easy to pay ransoms in 2022. A 2017 AEP group observed that the difficulty of using cryptocurrency was "a primary constraint on the success of the ransomware business model."[vii] There has been insufficient policy focus on often US-based **professional ransom intermediaries** that have sprung up in recent years—like Digital Forensics and Incident Response companies (DFIRs), cyberinsurance companies (CICs), and law firms— that provide US and foreign ransomware victims easy dollar on-ramps to cryptocurrency ransoms. Additionally, USG has worked with international partners to deter ransomware gangs by arresting and extraditing Ransomware-as-a-Service (RaaS) affiliates and shutting down servers. Asset seizures reduce profitability and may deter criminals but returning ransoms to victims who choose to pay creates an incentivize for future ransom payments. USG should allocate resources to incidents based on societal impact, not ransoms; victim reimbursement should focus on damages.

Section III addresses the visibility of ransomware attacks: FinCEN reporting by financial institutions (FIs); reporting via StopRansomware.gov; CISA reporting mandate; "9-1-1 for ransomware." **Section IV describes the ease of paying ransoms** due to professional ransom intermediaries, including DFIRs, CICs, and law firms, alongside broader adoption of cryptocurrency. **Section V** discusses **incentives to defend or pay** and entities below the "cybersecurity poverty line," while **Section VI** analyzes how **ransom seizures** influence both victims' and criminals' incentives. **Section VII** covers **case studies** on USG actions against

ransomware: FinCEN and OFAC advisories; sanctioning cash out; arresting and extraditing RaaS affiliates; Midwestern college bankrupt after Iranian attack; "Maui" ransom claw back.

II. Key Points

1. USG should leverage existing ransomware reports to provide a complete picture. FinCEN received SARs on about half to three-quarters of ransom payments in 2020, far more than what Congress described as "artificially low reporting" to FBI (via IC3), or to CISA.[viii,ix] OFAC advises victims to report to LE to mitigate sanctions risks. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 mandates CI entities report both ransomware incidents (72h) and ransom payments (24h), but FinCEN, CISA, FBI, and others could begin to cross-reference ransom reports to identify as many ransomware incidents as possible without waiting for the mandatory reporting regulations. The Act also "requires the CISA Director to share and coordinate each report;"[x] we propose a "9-1-1 for ransomware" framework.

2. Ransomware is financially motivated, but ransoms alone are the wrong metric. Ransom payments are useful for identifying incidents but underplay the threat: e.g., 2019 estimated damages were 30 times larger than ransoms.[xi,xii] Ransomware "is economically destructive and leads to dangerous real-world consequences that far exceed the costs of the ransom payments alone,"[xiii] and "can spill over from the initial target to economically linked firms."[xiv] Downtime, delayed payroll, and supply chain disruptions occur regardless of ransom payment. LE should triage attacks based on damages and CISA prioritization of CI Sector.[xv]

3. Policies addressing ransom payment strategies ("cybersecurity poverty line"[xvi] and "plan to pay") can help reduce the overall threat. When victims cannot afford or choose not to invest in defense, they make easy targets and incentivize attacks. CI entities that cannot afford defense pay, go bankrupt, or both. USG offers some grants and free cybersecurity tools to entities in this situation and should consider additional efforts.[xvii] CI entities that can afford defense still weigh expected costs and effectiveness of defense against expected cost and odds of a successful attack, with some still determining that it is cheaper to plan to pay.[xviii,xix] Policy responses should consider how to tip the scales toward defense, not paying.

4. Asset seizure should be secondary to disruptive actions and consider incentives. US and international partners have seized funds from ransomware gangs and related criminal organizations while arresting criminals and seizing servers, which is a model for effective deterrence. Returning ransoms to victims does not enhance deterrence and creates a moral hazard. An expectation of ransom recovery will lead more victims to pay ransoms, incentivizing future attacks. Seized assets could compensate non-paying victims based on damages, aligning victims' incentives with national security goals and USG advice not to pay. Focusing on seizure rates may lead to misallocating resources based on ransoms, not damages;[xx] metrics should include total attacks and payment rate when attacks succeed.

5. Ransomware is cryptocurrency-enabled but involves professional ransom intermediaries. Ransoms rarely start as cryptocurrency. Funds typically flow from victims to intermediaries

to cybercriminals, involving multiple fiat transactions. FinCEN's Advisory outlines this flow of ransom funds, but almost all other analyses we reviewed elided the role of professional ransom intermediaries. These intermediaries pose a risk of regulatory capture, with intermediaries leveraging their role in providing visibility on ransomware incidents to USG to shape policy even as they play a key role in the financial ecosystem enabling ransomware.

2022 PUBLIC-PRIVATE ANALYTIC EXCHANGE PROGRAM

TEAM INTRODUCTIONS

MEMBERS	COMPANY
Kim Anstett	Iron Mountain
Nicholas Gaydos	Duke Energy
Timothy Krugh	UPS
Kelsey M.	NCTC Cyber
Sallie Newton	Intel
Matthew S.	FBI
Chad Ratashak	Wells Fargo
Krista V.	New Jersey Cybersecurity
Susan W.	DHS
Champion	*Champion Agency*
Derek B.	*NSA*
Shannon Q.	*DHS – USCIS*

Glossary of Terms

Bank Secrecy Act (BSA)

Anti-money laundering (AML)

Bitcoin (BTC)

Critical Infrastructure (CI)

Cyberinsurance company (CIC)

Cybersecurity and Infrastructure Security Agency (CISA)

Department of Justice (DOJ)

Digital Forensics and Incident Response company (DFIR); our focus is on DFIRs that facilitate ransoms, as described in FinCEN's Ransomware Advisory

Doxing: publishing sensitive data with malicious intent

FBI Internet Crime Complaint Center (IC3)

Federal Bureau of Investigation (FBI)

Financial Crimes Enforcement Network (FinCEN)

Financial institution (FI)

Law enforcement (LE)

Monero (XMR)

Money services business (MSB)

Ransomware-as-a-Service (RaaS)

Small- and Medium-Sized Businesses (SMBs)

Suspicious Activity Report (SAR)

U.S. Department of Homeland Security (DHS)

U.S. Department of the Treasury (Treasury)

U.S. Department of the Treasury Financial Crimes Enforcement Network (FinCEN)

U.S. Department of the Treasury Office of Foreign Assets Control (OFAC)

United States dollar (USD)

US Government (US

III. Visibility: Identifying Ransomware Incidents and Payments

The US Congress, Treasury, CISA, DOJ, and others have emphasized the importance of improving the visibility of ransomware attacks, particularly attacks on critical infrastructure, including through mandates and voluntary reporting. USG may already be "seeing reports of ransomware incidents slow down or even decrease,"[xxi] which may be driven by fewer reports rather than a decline in underlying incidents. Therefore, USG should identify new ways to detect incidents and improve current and future reporting streams. This section describes ways that USG and private sector intelligence can identify ransomware incidents and payments without relying on professional ransom intermediaries (see Section IV) or offering to return ransoms to cooperative victims that choose to pay (see Section VI).

> "The government is largely in the dark when it comes to the scale of ransomware attacks pummeling schools, local governments and businesses…"— HSGAC quoting *Washington Post*[xxii]

A. Reporting mandates and incident reporting process

- OFAC guidance encourages ransom payment reporting to mitigate sanctions risk.
- New legislation will require CI entities to report payments (24h) and incidents (72h).
- Other regulators may have additional reporting requirements based on CI Sector.
- CISA's StopRansomware.gov is meant to be a one-stop shop for ransomware.[xxiii]
- FBI's IC3 receives some ransomware incident reports, but far less than FinCEN.

B. Third-parties could report attacks on critical infrastructure if there were a clear process

- An FI may know when a customer is a ransomware victim but has not paid a ransom.
- A ransomware attack on critical infrastructure may have knock-on effects that make economically connected entities, employees, and customers aware of the attack.

C. Open-source intelligence (OSINT) and blockchain analytics.

- Bitcoin public ledger can be analyzed with OSINT.
  - Ransomware gangs began demanding Monero to mitigate this transparency.
  - Monero has low liquidity mainly provided by professional ransom intermediaries.[xxiv]
- Blockchain analytics firm can tally ransoms.
- Cybersecurity firms can analyze doxing websites.

D. Suspicious Activity Reports (SARs) to FinCEN:

- CISA should compare incident reports with FinCEN's ransom reports and OSINT.
- Banks should file SARs on ransom-related payments, e.g., victim's bank, intermediary's bank, and centralized cryptocurrency exchange's (CEX's) bank.
- Professional ransom intermediaries, like DFIRs and CICs that facilitate or reimburse ransoms, should file SARs on ransom-related payments.
- CEXs should file SARs on ransom-related payments.

A. Mandatory Victim Incident Reporting: Sanctions, Regulations, and Recent Legislation

OFAC Reporting Guidance. OFAC's Updated Ransomware Advisory notes that "OFAC will consider a company's self-initiated and complete report of a ransomware attack to law enforcement or other relevant U.S. government agencies, such as CISA…made as soon as possible after discovery of an attack, to be a voluntary self-disclosure and a significant mitigating factor in determining an appropriate enforcement response."[xxv] Strict liability applies to sanctions violations including ransom payments. While the advisory only applies to ransoms that violate sanctions, it is almost impossible to be certain (e.g., reevaluation of sanctions with ransom payments to Conti after the "Conti Leaks" revealed ties to the FSB).

Mandatory Reporting Legislation. The Cyber Incident Reporting for Critical Infrastructure Act of 2022, introduced with bipartisan support by the U.S. Senate Homeland Security & Government Affairs Committee (HSGAC) Chairman Peters and HSGAC Ranking Member Portman, was an important step in addressing ransomware. The legislation requires CISA to create implementing regulations for 72-hour cyber incident reporting and 24-hour ransom payment reporting. More recently, both the HSGAC Majority Staff Report prepared for Chairman Gary Peters ("the Peters Report")[xxvi] and the HSGAC Staff Report for Ranking Member Portman ("the Portman Report")[xxvii] recommended swift implementation of the new ransomware incident and ransom payment reporting mandates.[xxviii,xxix] We agree that CISA should implement reporting requirements, but note that it is already in the self-interest of all victims who pay a ransom to report the incident to LE to mitigate sanctions risks.

SEC. In March 2022, SEC Chair Gary Gensler released a statement on a proposed cybersecurity disclosure mandate for public companies.[xxx] The mandate would have two components. First, "mandatory, ongoing disclosures on companies' governance, risk management, and strategy with respect to cybersecurity risks." The strategy disclosure includes "management's and the board's role and oversight of cybersecurity risks; whether companies have cybersecurity policies and procedures; and how cybersecurity risks and incidents are likely to impact the company's financials."[xxxi] Second, timely disclosure of "material cybersecurity incidents [that] could indirectly benefit external stakeholders such as other companies in the same industry…"[xxxii]

Under the first mandate, public companies may have to disclose that their cybersecurity strategy is "plan to pay" (see Section V). Mandatory disclosure would make the "plan to pay" strategy riskier for a public company, because public knowledge that the firm's ransomware recovery plan involves paying the ransom would place that firm at greater risk of attack. However, since the plan to pay strategy puts other companies at risk as well, this result may improve national security by discouraging companies from planning to pay. SEC should coordinate with CISA and other USG agencies to make sure these mandatory disclosures align with the overall counter-ransomware strategy. The second mandate has received criticism from industry by forcing companies to make disclosures while incidents may still be ongoing, undermining their security and incident response.[xxxiii]

Sector Risk Management Agency: TSA Example. Certain critical infrastructure entities may have additional sector-based obligations to report "data breaches" or "cybersecurity incidents," which may include ransomware incidents. In July 2021, TSA issued a directive placing cybersecurity requirements on critical pipeline owners and operators, including reporting confirmed incidents to CISA.[xxxiv] TSA issued a directive in December 2021 requiring rail owners and operators to report cybersecurity incidents to CISA within 24 hours.[xxxv] When implementing the mandatory reporting legislation, CISA should work with Sector Risk Management Agencies to standardize reporting timelines unless there is justification for sector-specific deadlines based on higher risk on CISA prioritization.

StopRansomware.Gov and Ransomware Reporting Difficulties. The Peters Report cautions against placing excessive reporting requirements on victims without a commensurate improvement in the reporting process and the dissemination of reports throughout the federal government.[xxxvi] Many victims have also expressed frustrations with the reporting process and the lack of USG response after an attack has occurred.[xxxvii,xxxviii] Launching StopRansomware.gov centralized informational resources on ransomware but it requires improvements to become a one-stop shop for ransomware incident reporting.

The "report" button currently overwhelms victims with numerous contact options. CISA's own reporting form, one option among many, appears intended for IT professionals and would be difficult for non-technical professionals. The page notes the victims may also report to several other USG agencies through various methods. Victims are in the early stages of an attack will be focused on mitigation and recovery, so reporting should be streamlined, as noted in the RTF Report and the Peters Report.[xxxix,xl] StopRansomware.gov should be revised to clearly direct victims to a simple reporting form that goes to CISA. The initial report form should be easy to complete within 24 hours of an attack and gather key details only. CISA can request more data, including damage estimates, once the attack is mitigated.

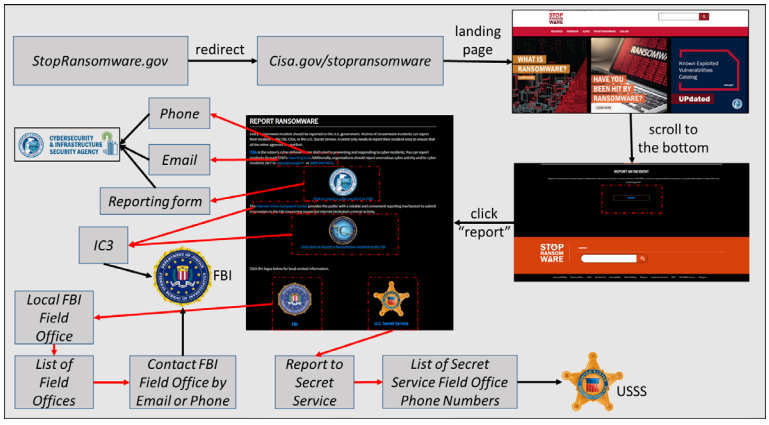

Figure 1. Diagram of current StopRansomware.gov reporting process.

> "The process for victims who are seeking to 'do the right thing' is confusing and expensive which works against U.S. national security interests." –Peters Report[xli]

CISA "9-1-1 for Ransomware." If an arsonist set fire to your home and injured your family, you would not be expected to call fire, medical, and law enforcement separately: you simply call 9-1-1 and a dispatcher coordinates the emergency response on your behalf. A victim's first contact with CISA should be more like the 9-1-1 experience. CISA could improve the online form and provide a hotline. After notification of a ransomware incident, CISA would be responsible for providing the information to the relevant parties: local police departments, state agencies, federal agencies, information sharing and analysis centers (ISACs), etc. These relevant parties would subsequently reach out to victims to provide resources and services, and request additional information, where applicable.

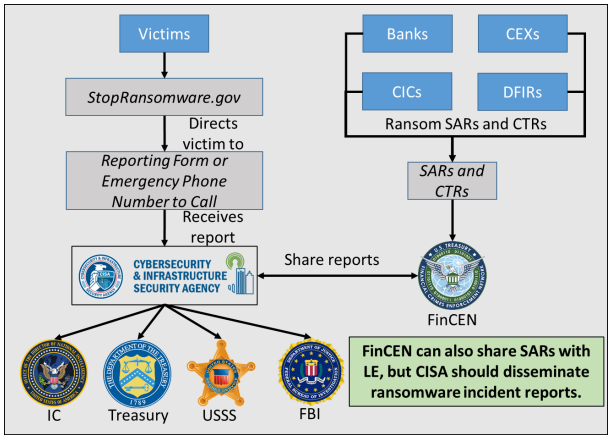

Figure 2. Suggestion for "9-1-1 for ransomware" framework.

B. Non-Payment Intelligence to Identify Ransomware Attacks on Critical Infrastructure

Ransomware attacks on critical infrastructure come to the knowledge of many entities beyond the primary target. Banks and other FIs may be aware of ransomware incidents that do not result in payment or indirectly impact their customers.[xlii] Private sector entities may be indirectly harmed by ransomware attacks on critical infrastructure. USG should address ways to gather non-payment and third-party incident reports, which would give USG higher odds of detecting a given incident and help estimate total damages from attacks on critical infrastructure including second-order effects.

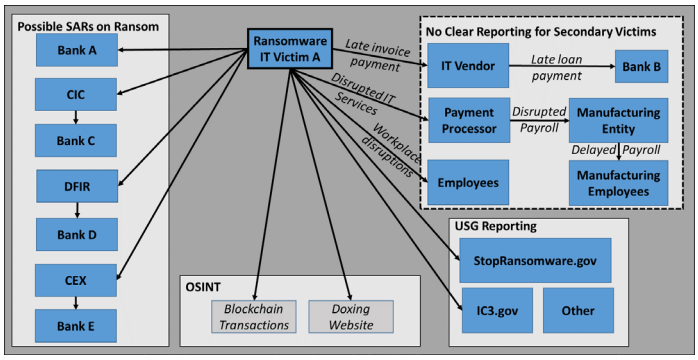

Figure 3. Possible ways USG could learn about a ransomware attack on Critical Infrastructure Entity Victim A.

For example, consider a ransomware attack primarily impacting an IT firm:

- **Bank A is aware that its customer, Victim A, a Critical Infrastructure Entity in the Information Technology Sector, was a victim of ransomware, but has not identified a ransom-related payment; employees of Victim A are also likely aware of an incident, though they may not know specifics.** FinCEN may consider using 314(a) to share information. USG should make explicit whistleblower protections for employees reporting ransomware incidents and create opportunities for reports.

- **Victim A did not pay vendor Victim B, also a CI entity in the IT Sector. Victim B missed a loan payment to Bank B due to the attack on Victim A.** Victim B or Bank B could notify USG of the attack on Victim A and the secondary supply chain damage to Victim B if there were a clear reporting stream.
- **Bank C is aware that Victim C, a Critical Infrastructure entity in the Financial Services Sector, had some of its IT systems infected by ransomware attacking primary target Victim A.** Victim C or Bank C could notify USG of the attack on Victim A and the secondary supply chain damage to Victim C if there were a clear reporting stream.
- **Bank D is notified by Victim D, a Critical Infrastructure Entity in the Critical Manufacturing Sector, that it is unable to process key payments, such as payroll, billing, or point-of-sale, because those systems are managed by Victim C.** Victim D or Bank D could notify USG of the secondary supply chain damage to Victim C and Victim D, although it would not necessarily know about Victim A, if there were a clear reporting stream.

C. Blockchain Analytics

Blockchain analysis allows LE to identify large ransomware payments without relying on reporting. DOJ's Ransomware Task Force noted that technology, such as blockchain analytics, can help identify and combat ransomware.[xliii] Blockchain analytics can provide OSINT on ransom payments, particularly very large ransom payments.[xliv] For example, LE could review Bitcoin "whale" transactions (greater than $1 million) to identify possible large ransom payments. LE could look for other indicators of ransom payments, such as high transaction fees (indicating intent to move money quickly), moving the funds through multiple unhosted wallets in a short period of time, connections to reused ransomware wallets, and transactions with darknet markets or high-risk exchanges. This could provide a check on unreported ransoms, as LE could cross-reference blockchain OSINT with reporting made under Treasury and CISA reporting guidance.

D. Identifying Ransom-Related Transactions

As long as the USG permits ransom payments, it should extract as much intelligence as possible from these payments; therefore, compliance with BSA/AML regulations is essential.

CISA and FinCEN Intelligence-Sharing. CISA and FinCEN should coordinate to combine cyber incident reports and ransomware SARs, respectively. CISA should disseminate this combined data to relevant parties, including the FBI field office near the victim, USSS, Treasury, and the IC, as well as the victim's Critical Infrastructure Sector Risk Management Agency. FinCEN would be responsible for sharing LE feedback on ransomware SARs with FIs. CISA could allow victims to fulfill the ransom reporting mandate by completing a CTR.

> "CISA must work with all possible partners to gain increased visibility into national risks. With increased visibility, we can better identify adversary activity across sectors, which allows us to produce more targeted guidance, understand the degree to which adversary activity

> across sectors is increasing risk, and identify particular incidents requiring a specialized CISA response team." –Eric Goldstein, Executive Assistant Director for CISA[xlv]

SAR Reporting to FinCEN. FinCEN encourages FIs to file SARs on ransom-related payments. This is not limited to the on-chain transaction sending BTC to the ransom wallet, but all the transactions from victim to criminal to cash out (see "Ease of Paying Ransoms"). All parties involved in the ransom payment process, including traditional banks, CICs, DFIRs, and CEXs, should also consider using 314(a) and 314(b) information sharing. We recommend that StopRansomware.gov provide more links to information regarding the financial reporting aspects of ransomware, such as AML regulations and sanctions risks for victims and FIs.

Currency Transaction Reports (CTRs). USG currently requires FIs to file a vast number of CTRs that LE does not use.[xlvi] The CTR threshold has not been adjusted for inflation since 1970, and, as noted in the Peters Report, rarely applies to ransomware payments because it does not apply to cryptocurrency.[xlvii] To address reforms to the CTR threshold, FinCEN should study the rate of LE inquiries about CTR reports and CTR evasion-related SARs, as recommended in AMLA 2020.[xlviii] Raising the CTR threshold and applying it to cryptocurrency could reduce the overall volume of CTRs while including nearly all ransomware payments.

DFIRs' intelligence value versus systemic risks. Intermediaries may provide payment intelligence to USG on ransomware gangs, but at the cost of a business model that enables a faster attack cycle and more complex money laundering. As noted above, intelligence on these incidents could be gathered through other means without relying on the entities that make the ransomware business model work. USG can gain intelligence on ransomware incidents—without relying on professional ransom intermediaries—through OSINT and blockchain analytics, SAR filing by banks and CEXs, and third-party and victim reports.

Policymakers should weigh the intelligence value of the professional ransom intermediary industry against the systemic risks caused by the easy ransom payments they provide (see "Ease of Paying Ransoms"). The USG should at a minimum apply strict regulatory oversight to these intermediaries, including MSB registration and SAR filing. USG should make it clear to cybersecurity firms that they may not act as ransom intermediaries without complying with BSA/AML regulations. USG should review the regulatory framework regarding professional ransom facilitation services by cybersecurity-focused law firms (sometimes called "breach coaches"), including attorney-client privilege and BSA/AML regulations.[1,2]

Ransomware gangs used to take time explaining to victims how to acquire and send Bitcoin, possibly requiring several days; now, ransomware gangs can offload this process to DFIRs, which quickly convert victims' funds into cryptocurrency ransoms. Since intermediaries

[1] See, e.g., Schwarcz, Daniel B. and Wolff, Josephine and Woods, Daniel W | 28 July 2022 | How Privilege Undermines Cybersecurity, which argues that "in their zeal to preserve the confidentiality of incident response efforts, lawyers frequently undermine the long-term cybersecurity of both their clients and society more broadly."
[2] The Portman Report (pgs. 12-14), includes an overview of the issues of attorney-client privilege and work product privilege in ransomware incidents.

handle the payment process, ransomware gangs can likely move on to the next victim more quickly. Because the ransomware gang is now dealing with technically sophisticated DFIRs instead of victims, they can demand more complex payments, including Monero (XMR), which is harder to track than BTC. It is unlikely that victims would be able to acquire XMR without intermediaries. DFIRs also inform victims of ransomware gangs' trustworthiness and negotiate lower ransoms;[xlix] this may be beneficial from the perspective of victims who choose to pay, but it is worse for national security by increasing victims' willingness to pay, incentivizing future ransomware attacks on critical infrastructure.

> "Currently [in 2017], the ability to purchase, buy, sell, and trade with cryptocurrencies requires a technical background. As user friendly interfaces are developed and implemented, it will become easier for unsophisticated illicit actors to use cryptocurrencies to their advantage. **Ease of use for cryptocurrency purchase by the average user is a primary constraint on the success of the ransomware business model** [emphasis added]."—*Risks and Vulnerabilities of Virtual Currency: Cryptocurrency as a Payment Method,* DHS AEP 2017[l]

IV. Ease of Paying Ransoms: Intermediaries Not Just Cryptocurrency

"Most ransoms are paid in bitcoin" is technically true but also glaringly incomplete. Cryptocurrency is an essential step in modern ransomware payments, but the overall process is more complex and could not occur in most cases without fiat transactions and intermediaries.[3] The Portman Report noted that this "niche market…did not exist a few years ago" and now includes "roughly a half-dozen ransomware negotiation companies;"[li] this is an underestimate, although it may be accurate in terms of only companies that have complied with FinCEN's MSB registration guidance. It is highly likely that professional ransom intermediaries enable more victims to pay ransoms more quickly, thereby making ransomware more profitable. Ransomware is cryptocurrency-enabled, but extorted funds typically do not start as cryptocurrency.[4] For example, over two-thirds of US healthcare organizations experienced a ransomware attack in 2021 and nearly two-thirds of those paid the ransom,[lii] yet it is unlikely that many hospitals own bitcoin (BTC), so how would a hospital that does not own BTC pay a ransom?

Figure 4.This standard explanation of ransom payments ignores that most victims do not own cryptocurrencies and do not know how to use cryptocurrencies to transact between unhosted wallets.

A. Step 1: The Hospital's Bank

[3] Our team also shared information about ransomware payments and cryptocurrency cash out TTPs with AEP Team "Combatting Illicit Activity Utilizing Financial Technologies and Cryptocurrencies."
[4] Even in instances where CI entities "plan to pay" by stockpiling Bitcoin (e.g., AEP 2017|*The Future of Ransomware and Social Engineering* | pg. 25), the stockpiling involves banks and a CEX to host the wallet.

The funds would likely start in the hospital's USD bank account with a domestic financial institution (FI).[5] The USD funds would be sent from the hospital's FI, typically via wire or ACH, to a professional ransom intermediary. For this reason, banks should note that they may have critical infrastructure customers that may be sending ransom-related payments from USD accounts, even if these banks do not offer cryptocurrency products and services.

Some victims may instead acquire cryptocurrency directly through a centralized exchange (CEX) and send the on-chain ransom payment themselves, but this is less common. A CIC may reimburse the victim for the payment to the intermediary or, alternatively, may pay the intermediary on behalf of the victim. If USG decided to ban ransom payments, it would be relatively straightforward from a technical perspective for banks to interdict payments to ransom intermediaries; however, paying the ransom is not illegal unless it violates sanctions, so this would require a policy decision from USG to coordinate the entire financial sector, not a unilateral decision to be made by FIs.

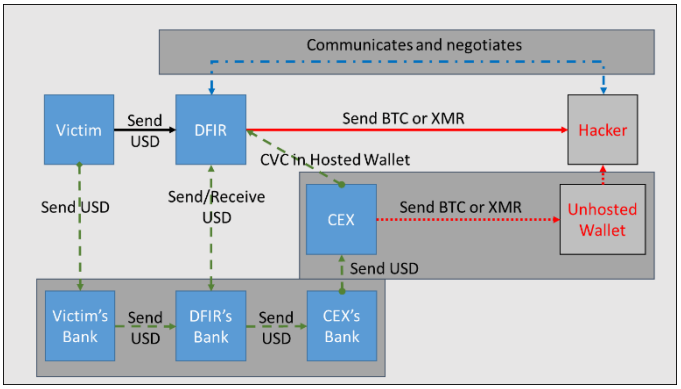

Figure 5. Model of a realistic payment process. Note that the Victim's Bank, the DFIR's Bank, the DFIR, the CEX's Bank, and CEX should all be filing SARs on the payment if they are aware that the payment is ransomware related. The victim should report the payment to LE or CISA to mitigate sanctions risks.

B. Step 2: The Hospital Hires a Professional Ransom Intermediary

The professional ransom intermediary would receive the funds. Common types are:

1. Digital forensics and incident response (DFIR) companies, which often portray themselves as cybersecurity or IT firms rather than financial institutions.
2. Cyberinsurance companies (CICs), which may have in-house DFIRs that facilitate ransoms or may reimburse victims for ransom payments made via DFIRs.
3. Law firms that facilitate ransom payments, sometimes known as "breach coaches," typically using Interest on Lawyers' Trust Accounts (IOTLA).
4. Other intermediaries may include Bitcoin lenders, tax preparers, and accountants.

FIs involved in ransom-related payments (in either BTC or USD) should be aware of applicable FinCEN and OFAC guidance regarding money services business (MSB) regulations for ransom intermediaries, SAR-filing guidance on ransom-related payments, and sanctions risks with strict liability. According to FinCEN's ransomware SAR trend analysis for 2021H1, DFIRs filed many SARs, but insurers filed few if any SARs, despite CICs' extensive involvement in ransom-related payments. While DFIRs filed many of the SARs that informed

[5] Many professional ransomware intermediaries are US-based, so foreign victims' (e.g. Australia, Canada, UK, EU) ransom-related payments may also be visible to US FIs.

USG of ransomware incidents, there are many other ways for USG to identify ransom payments without reliance on these entities.

Domestic FIs may be banking ransomware intermediary customers, such as DFIRs, without understanding the risks of their business model. This is particularly true of DFIRs that portray themselves as being in industries with low AML risk like IT and cybersecurity, when they are in fact operating as MSBs[liii] who send ransom payments to cybercriminals.

C. Step 3: Purchasing Cryptocurrency

The ransom intermediary would acquire BTC or another cryptocurrency. This typically involves a USD transaction between the intermediary's bank and the cryptocurrency exchange's bank. Therefore, the ransom in this scenario involved five FIs before USD was converted to BTC: three different domestic banks, an intermediary FI, such as a DFIR or CIC, and a centralized cryptocurrency exchange (CEX). The CEX would then credit the ransom intermediary's account with the equivalent amount of BTC. As noted below, it is highly unlikely that victims could acquire Monero in large quantities without intermediaries.

D. Step 4: Sending the Ransom On-Chain

The intermediary would send the BTC from the CEX, either directly to the unhosted ransom wallet or to the intermediary's unhosted wallet before being further sent to the unhosted ransom wallet. Unhosted wallets are self-custody wallets controlled by knowing the cryptographic private key and not "hosted" by a cryptocurrency exchange. The ransomware gang would then provide the decryption keys to the victim. Later in this paper, we discuss why "interdiction" of the ransom at this stage does not make sense in and offer alternative recommendations for seizures and blocking ransoms.

E. Step 5: Cryptocurrency Money Laundering On-Chain

The ransomware gang may launder the ransom on-chain using a variety of TTPs including peel chains, "chain hopping" between cryptocurrencies, and mixers. Sometimes, ransomware gangs do little to obfuscate the flow of funds on-chain, which anyone can follow on the BTC blockchain using free OSINT techniques or paid blockchain analytics.[liv,lv,lvi] The use of XMR and other AECs makes tracing extremely difficult. However, AECs have low liquidity in the U.S. and policymakers could address the AEC threat by banning ransom intermediaries for using AECs, possibly through sanctions or other financial regulations. It is highly unlikely that victims would be able to covertly source AECs themselves for six- or seven-figure ransoms without professional ransom intermediaries.

F. Step 6: Cashing Out

The ransomware gang will most likely attempt to cash out that majority of the funds by transferring the cryptocurrency from unhosted wallets to wallets controlled by high-risk exchanges and darknet markets, in exchange for various national currencies or precious

metals. Cash-out operations serving ransomware gangs may overlap with other criminal activities, such as illicit drug trafficking and child exploitation. Therefore, tracking ransom payments may lead USG to professional money laundering operations linked to other crimes that are harder to detect. Most recent USG actions, including by OFAC and LE, have focused on cash-out operations, including Suex, Chatex, Garantex, and Hydra Exchange (see "Case Studies"). USG has also worked with international partners to improve cryptocurrency regulations in countries like Estonia, which was previously a popular location to register CEXs cashing out Russian ransomware gangs.

G. Should it matter what technology is used to pay?

> "Wherever possible, regulation should be 'tech neutral.'" –Treasury Secretary Yellen[lvii]

Current ransomware policy discussions are disproportionately driven by a focus on the technical aspects of cryptocurrency, rather than "tech neutral" rules for ransom payments. USG policy permits ransomware payments via cryptocurrency with few restrictions, inconsistent with the zero-tolerance approach toward similar payments that incentivize criminal behavior like corruption[lviii] and terrorist kidnapping.[lix] Professional ransom intermediaries operate freely in the US, transferring ransom funds to cybercriminals as a standard business service.

Regulations related to ransomware payments should, in theory, apply based on the activity not the technology. However, consider if each of these processes would be treated in the same way:

1. Victim sends USD to an intermediary (e.g. DFIR or CIC) who sends BTC to the hacker.
2. Victim sends a wire to a company controlled by the hacker in a safe haven country.
3. Victim pays an intermediary to ship bulk cash to the hacker in a safe haven country.

Why should US ransomware policy favor ransom payments in cryptocurrency over those paid via wires or cash? Tech neutral rules should either ban or allow all three scenarios. As long as intermediated ransom payments are considered a legal business decision, policy discussion should focus on the legality of ransom payments and regulating the professional ransom intermediary industry, rather than technical details about the blockchain, mixers, or Monero.

Treasury has clearly stated that "Russia is a haven for cybercriminals,"[lx] but OFAC has not recently sanctioned specific ransomware gangs. Paying ransoms to cybercriminals in Iran or North Korea would be illegal due to jurisdiction-based sanctions, but despite heavy sanctions on Russia, it is still technically legal for victims to pay ransoms to most Russian ransomware gangs. At the same time, it is very difficult to pay for most goods and services from Russia without navigating a variety of special licenses from OFAC and sanctions on

Russian FIs. Isolating most of the Russian economy—but not banning ransom payments to Russian cybercriminals—may incentivize high-skilled Russian individuals to move from legitimate industries to ransomware gangs.

V. Defend versus Pay

The strategic situation for ransomware is like a Prisoners' Dilemma: if no one paid ransoms, ransomware attacks would diminish significantly.[6] However, it is often in the real or perceived self-interest of each victim to pay the ransom (see also "Appendix E: Cybersecurity Cost-Benefit Analysis"). Paying ransoms leads to future ransomware attacks. Potential ransomware victims in critical infrastructure may adopt a variety of strategies related to defending or paying ransoms. Some victims may make strategic miscalculations; we can address these sub-optimal strategies primarily through education on the real risks of ransomware and on cyber hygiene. Other victims may pay or plan to pay ransoms based on rational self-interest calculations, which results in an undesirable outcome from a whole-of-society perspective, because these entities' choice to pay likely encourages future ransomware attacks on critical infrastructure. Even NIST standards discuss cost-effectiveness in cybersecurity controls.[lxi] However, this may be distorted by incomplete information, underestimating damages, or assuming there are "bigger fish to fry."

A. Addressing sub-optimal strategies with education and planning

Some victims of ransomware may underinvest in defense or pay ransoms based on flawed reasoning. When the victims' choices are a mistake, rather than self-interest, educating potential victims can lead them to realize that investing more in defense or refusing to pay ransoms is in their own self-interest, aligning their actions with national security goals.

- **Bigger fish to fry: underestimating risk profile.** A company may underestimate the odds of becoming a victim of ransomware, resulting in underinvestment in cybersecurity. For example, repeated reference to a few major incidents in studies, reports, and media coverage may lead SMBs in CI Sectors to assume that ransomware is rare and only hits big targets, when ransomware is common and constantly hitting SMBs, e.g., RTF data showed around 3,000 US ransomware attacks in 2021, half against entities with 200 or fewer employees. Educating victims may lead them to invest in defense based on a more realistic understanding of the frequency of ransomware attacks. We encourage quantitative and qualitative research that provides perspective by discussing diverse ransomware incidents (e.g., the Portman Report case studies, reports by RTF and Sophos, and *The Ransomware Files* podcast), instead of rehashing the same handful of examples.

[6] The game theoretic analysis of ransomware strategies is far more complex since victims know other victims will pay, but from a whole-of-society perspective, the initial challenge comes from whether victims will pay.

- **Panic payments.** Some companies may pay ransoms out of panic when they do not need to, either because they have prepared to mitigate and recover, or because there may be outside help.[7] For example, the IT team made substantial backups, but the CEO was not aware and authorized a payment; companies can conduct tabletop exercises and document ransomware incident response to avoid this situation. There have also been situations when LE or private researchers had a decryptor for a ransomware variant, which allowed free decryption if the victim had notified LE.[lxii]
- **Underestimating the cost of the ransom payment strategy over other strategies.** When making a cost-benefit analysis of whether to pay or defend, a victim company may underestimate how much a ransom will cost or incorrectly assume that paying the ransom is equivalent to preventing the attack in the first place. In fact, some attackers do not provide decryption keys through malice or because the attacker is not truly financial motivated (e.g., the NotPetya "ransomware" attack);[lxiii] this points to a related principle, which is that improving defense helps regardless of attacker motives, whereas "plan to pay" only helps against financially motivated attackers. Decryption keys may work slowly, and data is usually lost, e.g., only 61% of data was recovered on average by victims who paid a ransom, according to Sophos, and only 4% of victims restored all data after paying.[lxiv] Decrypting data also does not address the underlying vulnerability. For example, an IAB may sell network access to a second ransomware gang, or the same gang may attack a few months later.

Increasing the likelihood of individual victims making ransom payments worsens national security. Professional ransom intermediaries, by providing a quick way for victims to pay ransoms, allow them to make rash decisions when it is not necessary to pay. Intermediaries make it logistically easy to pay. Intermediaries increase victims' confidence in the likelihood of receiving decryption keys from a ransomware gang, making them more willing to pay a ransom than if they had doubts about the ransomware gang's trustworthiness.

B. When the rational choice is to pay

The benefit of not paying ransoms is diffused across all potential victims of ransomware, while the cost is borne by the victim alone. Therefore, victims are sometimes correct to determine that paying a ransom is their best choice even though it is worse for other potential victims. To resolve this issue, USG could ban payments, as it has with bribery and terrorist kidnapping, although this may be difficult, and the RTF report called for specific steps to be considered before implementing a ban.[lxv] Since victim ransom payment is an undesirable national security outcome, USG actions should consider changing incentives in situations where education is not sufficient, unlike the scenarios described above.

[7] "88% of executives from companies that have previously been hit by ransomware said they would pay if attacked again," according to Kaspersky, implying that about one in ten would not.

- **Below the cybersecurity poverty line: unable to pay, so hope for the best.** Some entities are so small or have such tight margins, that it is simply not practical to spend enough money to pay for adequate cybersecurity. These entities may be trapped in a situation in which a ransomware would likely result in the business having to close, yet they lack sufficient resources to defend. These entities may simply be hoping nothing bad happens to them and will either pay a ransom or go bankrupt, depending on the severity of ransomware attack. USG should consider possible ways to subsidize these entities, such as with grants to small CI entities or with incentives for CICs to provide coverage to these entities. Additionally, the tax code could be modified to provide more favorable treatment of business expenses on defense against ransomware, like data backup and recovery or improved network security, e.g., cybersecurity-as-a-service can be deducted as an operational expense, but a cybersecurity device could only be depreciated over several years as a capital investment. If regulators mandate investments in controls, it would make sense to allow businesses to deduct the costs immediately as an incentive.
- **Plan to pay.** Some entities have the resources to pay for cybersecurity but based on their expected value from the odds of becoming a victim and the cost of a ransom, plan to pay as the cheaper option, rather than plan to defend, mitigate, and recover. USG should carefully consider its actions and policies to discourage the plan to pay strategy while incentivizing defense, mitigation, and recovery.

When victims plan to pay, it is a worse outcome for national security. Cyberinsurance policies that cover the ransom make victims more likely to plan to pay, but this is becoming less popular as the costs of coverage have increased.[lxvi] Overall CICs appear to be moving toward more limited coverage, higher premiums, and higher underwriting standards. USG asset seizure policy could replicate the mistakes of cyberinsurance ransom coverage if the policy does not consider the impact on victims' incentives (see Section VI).

C. Cyberinsurance Underwriting Standards

Significant changes have occurred in the cyber insurance space in just the last year. The cyber insurance market is still in its infancy and, as such, adjustments are needed as the industry gathers more data on the cost to insure clients, while considering ransomware and the overall cyber threat landscape. In the last 24 months, premiums have been increasing significantly, with some clients experiencing premium increases[lxvii] of 100-300%. In addition to rising premiums and deductibles, cyber insurance providers are implementing minimum requirements for cybersecurity controls and best practices prior to issuing a policy, and in some cases, even prior to providing a quote to a potential client. While these changes will make it more difficult for some organizations to receive coverage, those that implement the requirements necessary to receive coverage will be more resilient to ransomware attacks.

The GAO recently released a study on applying the Terrorism Risk Insurance Program (TRIP)—the government backstop for losses from terrorism—to cyberinsurance in light of

ransomware attacks on critical infrastructure.[lxviii] This is an interesting area for future policy discussions, but USG policy should acknowledge that ransomware is financially motivated, unlike terrorism. Helping insurers remain solvent after terrorist attacks does not incentivize future terrorist attacks but providing a backstop for CICs could exacerbate ransomware. A TRIP-like program for cyberinsurance should prohibit coverage for ransom payments and should be crafted to make sure CICs maintain high underwriting standards.

Historically, organizations with cyber insurance were considered valuable targets for ransomware threat groups, as they operated under the assumption that insured victims are more likely to pay ransom demands; however, in the coming years, those with cyber insurance may be less likely to be targeted as their networks will be better hardened after implementing the controls now required by CICs, in addition to the growing resistance to paying cybercriminals. The changes may make it harder for SMBs to receive cyber insurance coverage in many cases due to the cost associated with better cybersecurity practices and rising premiums and deductibles. We may see ransomware threat groups shift focus to those entities, and begrudgingly accept smaller ransom amounts to ensure they will be paid. SMBs generally have slimmer profit margins and are often unable to devote adequate funding for cybersecurity, increasing the likelihood of targeting. SMBs are also more likely to go bankrupt due to ransomware attacks, which could lead to market concentration; market concentration, in turn, could increase the systemic risk of future ransomware attacks.

VI. Fighting Ransomware Financing Through Asset Seizures: No Refunds

DOJ has stated that its two main goals in combating ransomware are an increased percentage of reported ransomware incidents (see Section III) and an increased rate of asset seizures.[lxix,lxx,lxxi] Asset seizures are effective at combating ransomware when they are in service of depriving cybercriminals of enjoying their ill-gotten gains or preventing them from funding future attacks. Returning ransoms to victims does not enhance deterrence and creates a moral hazard. The decision to pay a ransom goes against USG advice has negative externalities for future victims. Ransom payments create incentives for future attacks and may enable future complex attacks.[8]

For the purposes of this paper, we provide the following definitions of asset seizures:

- **Interdiction:** blocking a ransom payment before decryption keys are received.
- **Claw Backs:** seizing a specific ransom tied to a specific victim after decryption.
- **Confiscation:** seizing ransomware-linked funds from cybercriminals or exchanges.

[8] Ransomware gangs attack all kinds of entities, including but not limited to critical infrastructure. As the NetWalker case study shows, ransomware gangs invest in improving their TTPs and malware. Therefore, to get "left of boom" for ransomware attacks on critical infrastructure, all ransom payments are relevant. Additionally, this data is already gathered by FinCEN and does not require additional reporting mandates.

> "The FBI does not support paying a ransom in response to a ransomware attack. **Paying a ransom** doesn't guarantee you or your organization will get any data back. It also **encourages perpetrators to target more victims** and offers an incentive for others to get involved in this type of illegal activity [emphasis added]."[lxxii]

Interdiction is tantamount to a ban on ransom payments (see Appendix B: Ransom Ban). **Claw backs** are likely to be counterproductive and subsidize victims' decision to pay (see Section VII.H Maui case study). The best model for seizures involves **confiscation** from ransomware gangs, RaaS affiliates, or cash-out operations while conducting other disruptive actions (e.g., Section VII.A-B, G, case studies on RaaS affiliate arrests and Hydra Market).

Going after cash out operations and specific cybercriminals has also resulted in larger seizures in than "claw backs."[9] Even if claw backs had a high rate of success—which they do not—the approach of returning funds to victims who choose to pay should not be a policy pillar for counter-ransomware efforts, because it prioritizes victims based how whether they paid ransoms rather than the damages the suffered or the priority of their CI Sector. LE should align its actions with its own guidance and not reward victims who choose to pay.

A. Interdiction and Ransom Bans: Policy not technology

The idea of interdicting cryptocurrency ransom payments improperly replaces a policy question (should victims be allowed to pay ransoms?) with a technology question (is it possible to stop a specific step in the ransom payment process?). Interdicting any step in the ransom payment process is tantamount to a ransom ban, so if it is a desirable goal, then blocking cryptocurrency transactions between unhosted wallets is the least practical way to accomplish that goal. Policymakers could require banks to block victims' ransom-related payments to DFIRs, prohibit CICs and DFIRs from facilitating cryptocurrency ransom payments, or ban CEXs from selling cryptocurrency to DFIRs and ransomware victims. However, this would effectively be a ransom ban and cannot be separated from a broader discussion on the legality of ransomware payments (see Section IV.G and Appendix B).

B. Claw Backs: Moral hazard and misallocation of resources

Claw backs create a moral hazard by incentivizing victims to pay ransoms, neglect non-paying victims, and have little to no deterrent effect on cybercriminals. If you subsidize something, you will get more of it. Claw backs are a subsidy for ransom payments like cyberinsurance reimbursement of ransoms, but without market forces and "skin in the game" to eventually rein it in.

The higher the perceived odds of getting money back, the higher the willingness of a victim to pay the ransom. Conversely, why should a victim refuse to pay a while USG policy is prioritizes victims who paid? Higher the odds of victim payment will lead to more, not fewer,

[9] E.g., compare amounts seized from NetWalker and Hydra Market to small seizures from Maui, DarkSide, and REvil tied to specific ransoms.

ransomware attacks.[lxxiii] Imagine two business owners were intimidated by the mafia to pay protection money; one pays, the other refuses. LE then seizes the protection money paid by the first victim and returns it, while ignoring the other victim, whose business was burnt down by a mafia arsonist. Claw backs work under the same logic and are not consistent with US national security goals related to securing critical infrastructure.

The primary reason FBI might consider a claw back policy is to incentivize victims to report incidents,[10] but as described in Sections III and IV, it is far easier to identify ransomware attacks resulting in payment—with or without the victim's cooperation—than incidents that do not result in payment. Therefore, to the extent allowed by law, DOJ policy should instead consider damage-based restitution to victims who report incidents, rather than ransom-based restitution. Congress may need to modify existing asset forfeiture and victim restitution laws to allow for seized funds to reimburse non-paying ransomware victims; in the meantime, it would be better for DOJ to hold the funds rather than to return them to victims, which incentives future victims to pay.

Publicizing claw backs has no deterrent effect on ransomware gangs but may cause a marginal increase in victims' willingness to pay. A few claw backs are unlikely to deter ransomware gangs, who are likely to have a more realistic view of the odds of claw backs than victims. On the other hand, USG promotion of a few unrepresentative claw backs[11] may lead a low-information CI Sector owner or operator to believe there is a high chance LE will claw back their ransom. This would increase their willingness to pay, which would outstrip LE's ability to conduct claw backs and make ransomware worse.[12] Additionally, if a victim is reimbursed for a ransom payment by a CIC and LE claws the ransom back, or if the price of BTC increases, there is a small possibility that the victim may even profit from the ransom payment itself, though but not after counting damages, based on cryptocurrency volatility.[lxxiv]

LE resources would be better spent on helping victims with incident response, especially those who refuse to pay. USG ransomware policy should prioritize victims who refuse to pay, because by refusing to pay, these entities do not incentivize and fund future attacks on other victims. Victims who plan not to pay are more likely to have taken measures to defend their critical infrastructure and restore operations, lessening the societal impact of attacks.

C. Attacking ransomware finances: letters of marque and reprisal and RaaS insider threats

We suggest taking advantage of the nature of unhosted cryptocurrency wallets to incentivize parties other than LE to attack the finances of ransomware gangs. Since many ransomware gangs hold their assets in unhosted wallets, they must hold their own private keys. Unless these gangs have perfect operational security, there may be ways for hackers or insiders to

[10] This potential justification for claw backs appears in the Maui case study, Section VII.H.
[11] FBI has made unfulfilled promises to victims to return payments, according to the Peters Report | pg. 41.
[12] Compare DOJ's goal of increasing ransom recovery to the rate of BEC fraud recovery. Freezing wires is inherently simpler for LE than seizing cryptocurrency, yet BEC fraud has continued to grow. Additionally, recovering BEC fraud funds does not involve the same risks of moral hazard as ransom recovery.

obtain those keys and steal the funds from sanctioned ransomware wallets. LE could set up "surrender wallets" where recovered ransom funds could be sent. The funds would then be awarded following a formalized verification process, analogous to privateers receiving transfers of ownership from admiralty courts after capturing ships. Since the funds would be sanctioned until surrendered to LE, hackers would not be able to bypass this legal process without remaining subject to sanctions.

Hacking back ransoms. Some cybersecurity professionals and national security analysts have advocated for hack-back legislation that would allow private sector companies to engage in active cyber defenses against their attackers, including by leveraging the Constitutional concept of Letters of Marque and Reprisal.[lxxv,lxxvi,lxxvii] "A letter of marque authorizes private parties to engage in conduct that, absent the letter, would be piracy."[lxxviii] However, others have expressed concerns about the risk of escalation or misattribution that could result in attacks on unrelated parties.[lxxix,lxxx] Therefore, we suggest as a possible approach for a small number of authorized parties permitted to hack sanctioned cryptocurrency wallets. Rather than a blanket authorization to conduct retaliatory cyberattacks, authorized parties would only be able to take actions to covertly obtain private keys and steal ransomware gang's cryptocurrency. The goals would be to deprive the ransom gang of funds and incentivize parties other than USG to handle seizures, so that USG could reallocate its limited resources to incident response, investigations, arrests, server seizures, and counterattacks that should not be conducted by private sector actors.

For example, after a ransomware attack, a cybersecurity firm with a Letter of Marque may go after funds held by a ransomware gang either for their own benefit or on behalf of victims. A US critical infrastructure entity may choose to pay a ransom to avoid long disruptions in critical services, but then hire a cybersecurity firm with a Letter of Marque to conduct operations to retrieve the funds. After infiltrating the ransomware gang's network, the cybersecurity firm may identify a private key or seed phrase that allows the firm to transact from the ransomware gang's unhosted wallets. The firm would then send the funds to the established LE surrender wallet and go through an established legal process to obtain the funds for themselves and the victim that employed the cybersecurity firm.

RaaS insider threat and defectors. RaaS affiliates may operate in safe haven countries, such as Russia, as well as countries that may arrest and extradite them, such as Canada or Estonia (see Case Studies below). Cyberattacks on ransomware gangs will tip them off to LE attention, which may be a concern when there is a chance of arrest but not when cybercriminals are unlikely to face trial in the US. Therefore, USG ransomware policy should acknowledge this distinction (see Appendix C: Ransomware is Geopolitical). For safe haven countries, USG policy should encourage RaaS insider threats and encourage defectors to steal funds and turn themselves in to the US or allies. This would deprive ransomware gangs of funds and sow distrust among cybercriminals.

For example, a Russian ransomware gang member may have physical access to a hardware wallet or handwritten private keys for unhosted cryptocurrency wallets. The ransomware gang member could send the funds to an LE surrender wallet and then physically defect to the US or a partner country at a consulate or border crossing. Following a formalized defection procedure, the defector would be debriefed and enter into a plea agreement. The ransomware defector may then receive a small portion of the funds sent to the surrender wallet (this would be an incentive for defectors to take as much as possible before defecting). Some individuals in safe haven countries may even attempt to social engineer their way into RaaS operations for the purpose of stealing these funds and gaining legal status in the US or an allied country; this threat may in turn make ransomware gangs more paranoid about taking on affiliates, which would undermine the RaaS business model.

VII. Case Studies: USG and International Partners

The case studies below describe USG and international actions against ransomware. The case studies also demonstrate various points made throughout this paper, such as cashing out, damages v. ransom amounts, sanctions risks, ransoms funding improved TTPs for future attacks, paying is not equal to defense, and examples of effective asset seizures.

A. Canadian NetWalker RaaS affiliate: U.S., Canada, and Bulgaria Collaboration[lxxxi]

The NetWalker ransomware variant that infected critical infrastructure entities including "municipalities, hospitals, law enforcement, emergency services, school districts, colleges, and universities" and NetWalker "specifically targeted the healthcare sector during the COVID-19 pandemic."[lxxxii] According to a US court, NetWalker had approximately 100 RaaS affiliates receiving about 5,058 BTC total; a Canadian NetWalker affiliate received about 1,864 BTC, over one-third of the total, with "dozens of victim companies across the world."[lxxxiii] He sent 224 BTC to NetWalker's leader to invest in malware improvements.[lxxxiv] The RaaS affiliate admitted that "his entire ransomware activities involved over 2000 Bitcoins;"[lxxxv] he also received funds linked to Sodinokibi, Suncrypt, and Ragnarlocker.[lxxxvi]

In early 2021, U.S. and Canadian authorities seized cryptocurrency and cash, Bulgarian authorities disabled a dark web ransom negotiation communications platform, and Canadian LE arrested the Canadian NetWalker RaaS affiliate.[lxxxvii] Canadian officials seized 719 BTC.[lxxxviii,lxxxix] When he was arrested in January 2021, he had about $790,000 in Canadian cash and $421,000 in his bank.[xc] He had cashed out, sometimes receiving bags ranging from $100,000 to $150,000 in exchange for his ransom-sourced BTC.[xci]

The RaaS affiliate, a former IT consultant for the Canadian government, was found guilty in Canada and extradited to the U.S., where he entered a plea agreement in June 2022.[xcii,xciii] In Canada, the affiliate was found guilty of infecting 17 victims with ransomware causing losses of at least CAD $2.8 million. The Canadian judge ordered restitution be paid to eight

victims ranging from $3,000 to $999,000.[xciv] In the US, the NetWalker RaaS affiliate's plea agreement only specifically described on Victim 1 in Tampa, FL in 2020; "the ransom demanded of Victim 1 was $300,000 in bitcoin, which Victim 1 did not pay. Victim 1, however, estimated having spent approximately $1.2 million to respond to the attack, contain its damage, and restore operations to normal."

B. Estonian RaaS affiliate caught due to unrelated past fraud[xcv]

According to statements by the DOJ, "many of the world's ransomware players began as fraudsters engaged in other types of online crimes, and this case demonstrates that their crimes will catch up to them." An Estonian national was arrested in Latvia and sentenced to 66 months in prison after pleading guilty in April 2021 to conspiracy to commit wire fraud. The individual operated a cybercriminal forum and specialized in "cashouts" (unauthorized bank account withdrawals) and "drops." Post-extradition investigation revealed that the individual was also involved in ransomware attacks resulting in at least $11M in ransomware, $53M in damages, and at least 13 ransomware victims including seven in the US. Some proceeds were converted to cash (over $200,000 seized), some were used to purchase luxury vehicles and jewelry, and physical devices storing passphrases to BTC wallets were worth approximately $1.7M at the time of seizure.

C. Midwestern college bankrupt after Iranian ransomware attack despite paying ransom[xcvi]

A ransomware attack affecting a college's IT systems for recruitment, retention, and fundraising occurred during a critical enrollment period in late 2021. The college reportedly paid a ransom to an Iran-based ransomware gang; this would be a violation of jurisdiction-based sanctions that could be mitigated if the victim disclosed to LE, per OFAC guidance. Despite paying the ransom, it took months to fully restore its systems. The college said it would require a multi-million-dollar bailout to continue operating. This demonstrates that paying ransoms does not always result in decryption and that the damage multiplier of ransomware can be high—a five-figure ransom resulted in millions of dollars in damages.

D. Treasury: FinCEN and OFAC 2020 Ransomware Advisories and 2021 Updates

On October 1, 2020, both OFAC and FinCEN issued advisories related to ransomware payments.[xcvii,xcviii] OFAC's original advisory warned of the sanctions risk of paying ransoms but did not address victim reporting to law enforcement. FinCEN's original advisory described the role of professional ransom intermediaries and noted that SARs should be filed on ransom-related payments, but it somewhat elided the role of these intermediaries in describing the flow of funds (see Figure 6). Both updated reports in 2021 improved on the originals: September 21 (FinCEN)[xcix] and November 8 (OFAC).[c] The updated FinCEN advisory provided a more detailed description of the ransom payment process, while the updated OFAC advisory brought more clarity to victims by noting that proper cyber hygiene and LE notification would be significant mitigating factors for sanctions purposes, which helped provide clarity to victims who may have remained silent due to sanctions concerns.

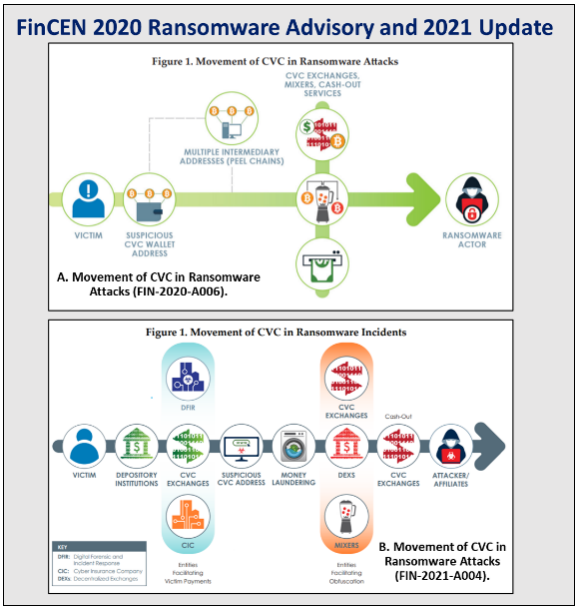

Figure 6. Chart showing ransomware payments. Updates made to FinCEN's 2021 Advisory significantly improved the chart by including banks and ransom intermediaries.

E. FinCEN AML/CFT Priorities 2021

> "The [eight] Priorities are, in no particular order: (1) corruption; (2) cybercrime, including relevant cybersecurity and virtual currency considerations; (3) foreign and domestic terrorist financing; (4) fraud; (5) transnational criminal organization activity; (6) drug trafficking organization activity; (7) human trafficking and human smuggling; and (8) proliferation financing." FinCEN AML/CFT Priorities 2021

After the passage of AMLA 2020, FinCEN released its first SAR Trend Report on Ransoms in 2021 and its first AML/CFT Priorities. The SAR Trend Report provided an excellent look at ransom reporting trends, but there has not yet been a follow-up report, so comparison over time is not possible. We encourage FinCEN to produce SAR Trend Reports on ransomware regularly and Congress may consider providing funding for additional staff tied to this goal. The AML/CFT Priorities included "cybercrime," but this category was dominated by discussions of ransomware; it is unclear why FinCEN did not simply say "ransomware," as "cybercrime" is vague. Ransomware attacks on critical infrastructure should be an AML/CFT Priority in the next report; in general, it would help regulated FIs take a risk-based approach if FinCEN picked fewer, more specific, ranked priorities. Additionally, Treasury's NMLRA should be aligned with FinCEN's AML/CFT Priorities and Ransomware Advisory.[ci]

F. OFAC Targets Cash Out Operations: Chatex, Suex, Chatextech, Hightrade Finance Ltd.[cii]

Since late 2021, OFAC has sanctioned several cryptocurrency exchanges linked to laundering the proceeds of ransomware, with Chatex as the common link. First, OFAC sanctioned Suex S.R.O. (registered Czechia but operated in Russia) in September 2021; this was the first-ever cryptocurrency exchange SDN.[ciii,civ] Suex operated as a "nested exchange" (trading on behalf of its clients using an account with a major exchange) using accounts with Binance and Huobi, according to *Coindesk*.[cv] The Suex designation coincided with OFAC releasing its Updated Ransomware Advisory. Second, OFAC sanctioned Chatex (Estonia), its website, cryptocurrency addresses, and related entities Chatextech SIA (Latvia), Hightrade Finance LTD (St. Vincent and the Grenadines), and Izibits OU (Estonia).[cvi] These SDNs were linked by Chatex and Suex websites, domain registration, Telegram channels, and beneficial ownership, according to TRM Labs.[cvii] The announcement of Chatex-related designations coincided with FinCEN releasing its Updated Ransomware Advisory.

Although the amounts were modest relative to overall ransomware volumes, ransomware-adjacent professional money laundering organizations appear to be experimenting with more complex TTPs. In late 2021, Chatex sent roughly $284,000 worth of cryptocurrency to NFT marketplaces according to Chainalysis.[cviii] OFAC sanctioned various Bitcoin and Ethereum wallets, a Tether wallet, and a Ripple wallet associated with Chatex. Review of the sanctioned Ethereum wallets identified transactions with ERC-721 and ERC-1155 tokens (NFTs) including art NFTs, metaverse "real estate" NFTs, and NFTs for blockchain trading card games and video games.cix One sanctioned wallet purchased an "Ethereum Name Service" (ENS) shortly before OFAC sanctioned Chatex. While reports continue to indicate that ransoms are sent to ransomware gangs almost exclusively in Bitcoin and Monero, the funds may be subsequently laundered on the Ethereum blockchain (ETH, ERC-20 tokens, and NFTs) and using stablecoins on various blockchains.

OFAC has done considerable work targeting specific ransomware cash-out operations, but it should provide a public report describing the strategic framework for its approach to ransomware, including entity-based and jurisdiction-based sanctions. The NMLRA 2022 mentions sanctions risks related to ransomware, including sanctions on Russia, North Korea, and Iran, and certain SDN ransomware gangs, like Evil Corp. However, the NMLRA 2022 does not contextualize these sanctions within its current policy. For example, OFAC does not appear to have sanctioned a specific ransomware gang since Evil Corp in 2019 and current policy seems exclusively focused on cash out operations. There may be good reasons for OFAC take this approach, but it is unclear why Treasury would tout old SDN listings of specific ransomware gangs if it has moved away from that approach.

Additionally, the *Treasury 2021 Sanctions Review* released in October 2021 never mentions "ransom" or "ransomware" and only mentions "cyber" once.[cx] This is particularly confusing, because OFAC had just released its Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments on September 21, 2021.[cxi] OFAC should explicitly address the role of ransomware sanctions in the overall sanctions policy toward Russia. If Russia faced jurisdiction-based sanctions like Iran and North Korea, this would effectively

make the vast majority of ransom payments illegal; given the rapid pace of Russian sanctions, OFAC should address this possibility before it happens.

G. OFAC Targets Cash Out with International LE and Regulators: Garantex and Hydra[cxii]

On April 5, 2022, OFAC added a high-risk cryptoexchanger GARANTEX EUROPE OU (GARANTEX EUROPE OÜ) in Estonia and Russia to the SDN list, along with the darknet market HYDRA MARKET in Russia.[cxiii] OFAC noted that Garantex operated out of Federation Tower in Moscow, Russia, like the earlier SDNs Suex and Chatex. In the press release, Treasury also frankly stated that "Russia is a haven for cybercriminals."[cxiv] Previously, in February 2022, the Estonian FIU had reportedly revoked Garantex's license and coordinated with Treasury in investigating Garantex. "Analysis of known Garantex transactions shows that over $100 million in transactions are associated with illicit actors and darknet markets, including nearly $6 million from Russian RaaS gang Conti and also including approximately $2.6 million from Hydra."

> "In coordination with allies and partners, like Germany and Estonia, we will continue to disrupt these [ransomware] networks." –Treasury Secretary Janet Yellen[cxv]

OFAC listed over 100 BTC wallets associated with Hydra. OFAC's investigation identified approximately $8 million in ransomware proceeds that transited Hydra's virtual currency accounts, including from Ryuk, Sodinokibi, and Conti. On April 5, 2022, German LE seized BTC and physical servers from Russian Hydra Market.[cxvi] Blockchain analytics firm Elliptic confirmed the German cryptocurrency seizures: 543.3 BTC worth $25.3 million at the time of seizure.[cxvii] After the SDN designation, DOJ indicted Dmitry Olegovich Pavlov for running the Germany-based servers via Russian company Promservice since 2015.[cxviii,cxix] Hydra Market laundered the proceeds of other illicit activity, including cryptocurrency linked to crimes, illegal drugs, stolen credit cards, exchange hacks, child sexual abuse materials (CSAM), scams, Ponzi schemes and frauds.[cxx]

H. Claw back of critical infrastructure ransoms paid to North Korean state-sponsored "Maui"

A joint FBI-CISA-Treasury alert in early July 2022 warned that North Korean state-sponsored cyber actors were using Maui ransomware to target the Healthcare and Public Health (HPH) Sector.[cxxi] A subsequent DOJ press release described claw backs in May 2022 of about $500,000 in ransoms to be returned to two HPH Sector victims.[cxxii] Seizing funds from Maui is a positive move, but returning the funds to victims who chose to pay increases risks to the HPH Sector and contradicts advice in the joint alert.

The goals of these claw backs, according to the DOJ press release, were to incentivize future victims to report and "to disrupt bad actors and prevent the next victim."[cxxiii] One hospital paid a ransom, then notified the FBI and cooperated with law enforcement, allowing the FBI to "identify the never-before-seen North Korean ransomware and trace the cryptocurrency to China-based money launderers."[cxxiv] While that information was apparently helpful to LE, there are alternative ways to identify ransom payments without victims' cooperation (see

Section III). Additionally, returning ransoms to victims does not "prevent the next victim" because it incentivizes payment, which incentivizes future attacks.

"The FBI, CISA, and Treasury **highly discourage paying ransoms** as doing so does not guarantee files and records will be recovered and **may pose sanctions risks.** [emphasis added]," [cxxv] yet the DOJ announced that the ransoms would be returned—despite sanctions on North Korea—undermining advice not to pay and warnings about sanctions risks. The DOJ mentioned "returning these funds to the rightful owners" and "work to successfully retrieve ransom payments where possible;" [cxxvi] however, this is inconsistent with discouraging ransom payments and centers policy on ransom amount when the key national security concern should be damages caused by ransomware attacks on critical infrastructure.

In the joint alert, the "FBI assesses North Korean state-sponsored cyber actors have deployed Maui ransomware against Healthcare and Public Health Sector organizations. The North Korean **state-sponsored cyber actors likely assume healthcare organizations are willing to pay ransoms** because these organizations provide services that are critical to human life and health**. Because of this assumption,** the FBI, CISA, and Treasury assess **North Korean state-sponsored actors are likely to continue targeting HPH Sector organizations** [emphasis added]." [cxxvii] By the same logic, claw backs likely make HPH Sector organizations more willing to pay ransoms, incentivizing future attacks on this CI Sector.

VIII. FORECASTS

- Ransomware may get worse before it gets better; but the hardening cyberinsurance market may improve the long-term outlook.
- Geographic diversification of the threat away from concentration in Russia and CIS.
- Possible rise in ideologically motivated ransomware "hacktivism."
- Terrorist organizations may obtain ransomware either through purchase of software, repurposing leaked source code, or becoming RaaS affiliates.
- Cyber and financial crimes investigations will require increased global cooperation.
- If more businesses begin to own and transact in cryptocurrency, this will significantly change ransom payment typologies.
- As more critical infrastructure becomes networked the attack surface will grow.
- The move by many companies to "the cloud" may have mixed results. Cloud companies may have better cybersecurity than SMBs, but they may also present a common point of failure for critical infrastructure entities (e.g., Kaseya attack).

ANALYTIC DELIVERABLE DISSEMINATION PLAN

Association of Certified Anti-Money Laundering Specialists (ACAMS), Association of Certified Financial Crime Specialists (ACFCS), Bank Policy Institute (BPI); Treasury, SEC, ONCD, Chainalysis, Elliptic, TRM Labs, CipherTrace, NCFTA, FS-ISAC, FSSCC.

DISCLAIMER STATEMENT: This document is provided for educational and informational purposes only. The views and opinions expressed in this document do not necessarily state or reflect those of the United States Government or the Public-Private Analytic Exchange Program, and they may not be used for advertising or product endorsement purposes. All judgments and assessments are solely based on unclassified sources and the product of joint public and private sector efforts.

Appendix A: Available Free Resources

Cybersecurity and Infrastructure Security Agency (CISA)

- Academic Institutions
- Federal Departments and Agencies
- Industry and Private Sector
- Non-Profit Sector
- State, Local, Tribal, and Territorial (SLTT) Governments
- Cybersecurity Grants

Multi-State Information Sharing & Analysis Center (MS-ISAC)

- Malicious Domain Blocking & Reporting (MDBR)
- Cyber Incident Response Team (CIRT)
- Cybersecurity Advisories
- Real-Time Indicator Feeds
- Cybersecurity Table-Top Exercise Templates
- CIS SecureSuite

Ransomware Task Force (RTF)

- Blueprint for Ransomware Defense: An Action Plan for Ransomware Mitigation, Response, and Recovery for Small- and Medium-sized Enterprises

Appendix B: Ransom Ban

Like the Ransomware Task Force's "A Note on Prohibiting Ransomware Payments," we found that finding consensus on a full ban is difficult. Banning ransoms would lower the incentives for ransomware attacks. However, "there remains a lack of organizational cybersecurity maturity" and ransomware attacks are low-cost, so "a prohibition on ransom payments would not necessarily lead them to move into other areas."[cxxviii] Therefore, our

team emphasizes recommendations that would incentivize more defense and less willingness to pay ransoms, while not taking the option to pay off the table in the short-term.

There are two reasonable objections to ransom bans that can be overcome through policy and LE actions. First objection: ransom bans will just push payments underground.[cxxix] As noted in Sections III and IV, most ransomware payments involve multiple entities other than the victim and are visible using blockchain analytics, so it would be extremely difficult for victims to pay ransoms, particularly six-figures and above, without professional ransom intermediaries. Even if some victims could still covertly source and pay ransoms on their own, this would be more time consuming and uncertain for ransomware gangs walking victims through the process, likely slowing down their attack cycle. Second objection: we simply do not have the technological capability to interdict cryptocurrency ransom payments. While that may be true in the future if critical infrastructure companies begin hold large amounts of cryptocurrency, most victims currently do not hold cryptocurrency and policymakers could prevent fiat on-ramps from providing easy ransom payments to victims.

We recommend three actions regarding ransom payments. First, make it harder for victims to plan to pay rather than to defend. While all types of professional ransom intermediaries make paying ransoms easier, thereby contributing to the problem, we assess that the cyberinsurance industry may play a constructive role due to "skin in the game" causing losses, which has led CICs to begin requiring higher underwriting standards. Conversely, intermediaries that only come in after an attack exacerbate the problem without encouraging defensive measures before the incident. Intermediaries that earn fees on a per-ransom basis have little incentive to reduce the overall ransomware problem. These intermediaries help the ransomware business model work. Policymakers should consider banning ransom intermediation absent a pre-existing relationship between the intermediary and the victim that aligns their incentives via exposure to shared losses when a ransomware attack is successful. This policy would likely result in CICs facilitating ransom payments as a last resort, but not other types of intermediaries. The goal would be lowering systemic risk caused by easy ransom payments by removing a key fiat on-ramp to the payment process.

Second, we recommend that LE not return funds to victims who choose to pay. Returning ransoms replicates the past mistakes of the cyberinsurance industry. Claw backs would encourage victims to pay in the future. Some of the ransom amount may have been used to fund subsequent attacks on other victims prior to recovery, causing damage to those victims for which they are not compensated under current "claw back" policy, which is not fair to those victims, nor does it align victims' incentives with national security goals. Third, if USG moves toward a ransom ban, we recommend that USG define an expanding ring-fence of organizations that would be prohibited from paying ransoms, similar to the factors in the RTF report.[cxxx] Start with a government ransom ban, first federal and then SLTT; next, implement a rolling ban by CI Sector on ransom payments and define credible retaliatory measures against ransomware gangs in a risk-ranking determined by CISA starting with the highest-

risked Sector; lastly, once all 16 CI Sectors are covered by a ransom ban, consider a blanket ransom ban based on criteria described in the RTF framework.

Appendix C: Ransomware is Geopolitical & "State Sponsors of Ransomware"

USG has compared the ransomware threat to terrorism. Congress should consider granting the State Department authorities to designate countries as State Sponsors of Ransomware, like the State Sponsors of Terrorism designation. For example, the Conti ransomware gang voiced support for the Russian invasion of Ukraine and threatened to overthrow the government of Costa Rica in a recent, massive ransomware attack on various government departments.[cxxxi] These actions demonstrate that ransomware gangs may align themselves with safe haven's strategic goals to maintain freedom of operation.

USG should work with international partners to create clear standards and norms around this designation and coordinate on punitive measures to discourage countries from operating as ransomware safe havens. Designating a State Sponsor of Ransomware would indicate that a jurisdiction is non-cooperative, so priority should be given to punitive and deterrent measures against ransomware gangs, with less priority given to investigations that are unlikely to result in extradition from the safe haven country. For example, the State Sponsor of Ransomware designation would be the basis for granting Letters of Marque and Reprisal to authorize hackers to steal funds from ransomware gangs.

The obvious challenge is that ransomware safe havens are also likely to be diplomatically and economically isolated nation-states, such as Iran, North Korea, Russia, or Venezuela, so differentiating punitive measures related to ransomware from broader actions against these countries may be difficult. Russia is a clear candidate for the first designation, although it would be difficult to tie punitive measures specifically to ransomware in light of sanctions related to the invasion of Ukraine. The US and allies should consider possible international legal norms to distinguish between ideologically motivated resistance groups from financially motivated ransomware gangs. For example, a ransomware gang attacking Belarus's train system for money would not be the same as the Belarussian "Cyber Partisans" hacking Belarus's train system to disrupt Russia's invasion of northern Ukraine.[cxxxii,cxxxiii]

In order to create international norms around ransomware, USG and its allies should suppress financially motivated ransomware gangs, even if they are attacking critical infrastructure in adversary nations. For example, the "NB65" ransomware gang is reportedly targeting Russian businesses.[cxxxiv] While ransomware gangs may use Russia's invasion of Ukraine for ideological cover, USG and allies should not permit the operation of financially motivated ransomware gangs in their own territory for several reasons. First, financially motivated ransomware gangs may turn their attention to Western targets in the future. Second, these groups may attack critical infrastructure, violating norms that USG wishes to

establish. Third, their victims are likely Russian civilian targets, not other ransomware gangs; as we recommend in Section VI, these groups could instead be incentivized to steal cryptocurrency directly from Russian ransomware gangs, rather than conducting destructive ransomware attacks on civilian critical infrastructure.

Appendix D: Ransomware and the FinCEN One Pager on AMLA 2020[cxxxv]

FinCEN's one-page summary of the AMLA 2020 highlights ten key requirements for FinCEN, including five that we identified as particularly relevant to combatting ransomware:

> 2. Establishing national anti-money laundering and countering the financing of terrorism priorities [...]
>
> 4. Reviewing, and revising as appropriate, Currency Transaction Report (CTR) and Suspicious Activity Report (SAR) reporting requirements, and other existing Bank Secrecy Act (BSA) regulations and guidance [...]
>
> 6. Codifying the FinCEN Exchange program [...]
>
> 9. Law enforcement reporting to FinCEN on the use of BSA data, procedures for additional feedback between FinCEN and financial institutions on the usefulness of SARs, and semi-annual publication of review of SAR activity and other BSA reports, including threat patterns, trends, and typologies; and
>
> 10. Codifying a pilot program to allow financial institutions to share SARs with their foreign branches, subsidiaries, and affiliates.

Regarding Key Requirement 2, we view the goal of establishing priorities to be very valuable. However, the first report in June 2021 describing the Priorities laid out in accordance with the AMLA 2020 is insufficient. There are too many Priorities, and each Priority is overly broad (see below for detailed critique).

We encourage FinCEN to use the authority provided in Key Requirement 4 to raise the CTR reporting threshold to allow regulated FIs to allocate AML resources more efficiently while applying the CTR requirement to almost all ransom payments. It may even be possible for FinCEN and CISA to coordinate on allowing critical infrastructure entities to tick a box for on an updated cryptocurrency CTR form that constitutes self-disclosure of a ransom payment. This would allow critical infrastructure victims or their agents (e.g., CICs) to satisfy the ransom reporting mandate via completion of the CTR while reducing the overall rate of CTRs, most of which go unused. Additionally, if victims disclosed that the purpose of the payment was a ransom via The CTR would be completed during the ransomware payment transaction and satisfy the 24-hour reporting requirement.

Regarding the second part of Key Requirement 4, we propose that FinCEN conduct a study to determine ways for FinCEN and FIs to share information when a customer is a victim of ransomware but does not pay a ransom and therefore a SAR filing would not be appropriate. For example, a bank learns that a local water utility was hit with a ransom demand but, as far as the bank knows from payment monitoring and the relationship manager, the victim has not paid the ransom. Perhaps a streamlined 314(a) process could be created for this type of reporting.

To date, FinCEN has hosted two FinCEN Exchanges on Ransomware.[cxxxvi] This is a valuable way to share intelligence on ransomware among "financial institutions, technology firms, third-party service providers, and federal government agencies."[cxxxvii] We support the formalization of this process, as described in Key Requirement 6. However, as noted elsewhere in this paper, we have serious concerns about the financial incentives motivating DFIRs and other ransom intermediaries. FinCEN should consider the impact that the presence of ransom payment negotiators and facilitators would have on other participants' ability to speak freely in future FinCEN Exchanges on Ransomware. We caution FinCEN to screen participants, including understanding their business models and incentives related to the ransomware payment ecosystem. Intermediaries with no relationship to victims prior to ransomware attacks who get paid to facilitate ransoms should be considered high-risk and receive the most scrutiny, compared to intermediaries like CICs that apply minimum cybersecurity underwriting standards and have "skin in the game" to reduce the overall frequency of ransomware attacks. FinCEN should reconsider the involvement of law firms if they are involved in the facilitation of ransom payments. All approved participants in FinCEN Exchanges on Ransomware should have mandatory disclosure requirements if they offer ransom negotiation and facilitation services.

Key Requirement 9 calls for LE feedback on SARs and other BSA data provided to FinCEN, which would be valuable for regulated FIs. LE feedback on the usefulness of ransomware SAR narratives and details provided would help FIs improve SARs to combat ransomware. Key Requirement 9 also calls for FinCEN to publish semi-annual reports reviewing the use of SARs and other BSA reports; however, it appears that FinCEN has only released two such reports: a report on Ransomware Trends in Bank Secrecy Act Data published in October 2021;[cxxxviii] and a report on Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data published in December 2021;[cxxxix] the latter only tangentially relates to the FinCEN AML/CFT Priorities. Going forward, FinCEN likely needs increased staffing to produce these SAR trend reports on a regular basis, but funding should also be contingent on requirements that FinCEN develop a more focused list of Priorities, act according to those Priorities, and consistently publish SAR trend reports on those Priorities.

Key Requirement 10 calls for a pilot program to allow domestic FIs to share SARs with foreign branches, subsidiaries, and affiliates. Ransomware would be an excellent topic for this pilot program. Ransomware is inherently international, with victims, RaaS affiliates, RaaS core members, and cash out operations all potentially operating in different countries.

Sharing ransomware SARs has a lower risk of "tipping off," because the information being shared would primarily be following the fiat on-ramps and off-ramps of ransom payments. US FIs could provide intelligence on victims' ransom payments because foreign victims sometimes pay US-based DFIRs to facilitate ransom payments, which are visible through correspondent banking relationships. Foreign FIs are more likely to be exposed to cash-out operations than domestic FIs (e.g., recent takedowns of exchanges and dark net market infrastructure in Czechia, Estonia, Germany, and Latvia).

Appendix E: Cybersecurity Cost-Benefit Analysis

For those in the cybersecurity industry that have never experienced a ransomware event firsthand it can be difficult to understand why companies would pay a ransom or may not invest in cybersecurity controls needed to protect against attacks. There are several reasons, but at its core cybersecurity is about balancing financial considerations with risk. Most company leaders are aware of the threat from ransomware and do not need to be convinced it is a business risk.[cxl,cxli,cxlii] Nor do they need to be told that they have vulnerabilities or that ransom attacks occur with great frequency. Most business leaders are aware of the risk, and in fact most are confident that their organizations are adequately prepared to handle ransomware attacks,[cxliii] although this may be skewed based on incorrect data as described in Section VI. The challenge for many companies, especially smaller and less regulated ones is:

1. The risk of a ransomware attack does not outweigh the cost of the required controls.
2. The cost of paying a ransom is less than the cost to recover without paying.
3. Companies may have no alternative other than insolvency.

Companies designated as critical infrastructure—such as energy, water, health, etc.—must now consider another: the immediate risk of loss of life and human health from a service disruption.[cxliv,cxlv] Double extortion ransomware attacks—data is stolen prior to encryption and victims are threatened with doxing if they do not pay—also introduces risks of lost trade secrets, compromise of sensitive PII, and lawsuits from angry customers and employees when their data hits the Dark Web.[cxlvi]

It is unclear if the rate of victims paying ransoms is improving. The situation may be improving, with only 46% of victims paid ransoms in Q4 2021 vs 85% in 2019, according to one DFIR.[cxlvii] However, another recent survey suggested that 88% of executives at companies previously hit with ransomware would choose to pay, indicating that they felt they had made the right decision for their company;[cxlviii] this implies perhaps one in ten may have "panic paid." This shocking statistic hammers home the cost-benefit analysis of those who have suffered a ransomware compared to those who have not. The challenge of telling companies to "invest in security," "not pay the ransom," and "recover and restore from

backups" is that companies many can plan to do this but may not have the choice once they suffer a ransomware attack.

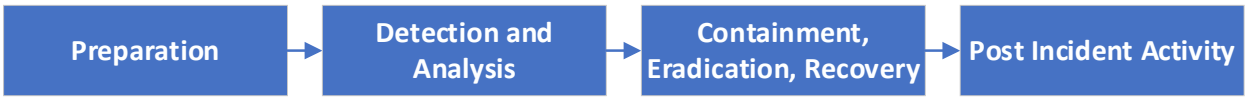

Figure 7. NIST Incident Response Process.

Preparation: Everyone has a plan until they get punched in the mouth

Governments, can provide non-excludable public goods, like national defense, that are funded by taxes, while businesses seek to generate profits for owners, regardless of whether they are publicly or privately owned or consider themselves "critical infrastructure" or "utilities."[13] When companies choose to not invest in security controls or hire competent staff, they accept, whether they acknowledge it or not, the risks tied with their actions. Likewise, when business decides to procure a manage security service provider (MSSP) or cyber insurance, they're transferring risk to another company, but may not fully understand[cxlix] the amount risk transferred and may have created new risks.[cl]

The cost-benefit analysis prior to a ransomware attack is rational based on perceived facts. This analysis continues when companies suffer to ransomware attacks albeit in a higher-stress environment. It is ultimately a profit-maximizing business decision whether to pay a ransom and how much to invest in cybersecurity. A company will not spend $20,000 to protect an asset that costs $10,000 and stay in business for long. Nor will a company pay $10 million in damages (disaster recovery costs, investigations, and business downtime) when a $1 million ransom will get the organization back up and running much faster and comparatively cheaper.

The level of formality of these cybersecurity risk analyses can vary widely between organizations. Some cost-benefit analyses may be based on rough heuristics, rather than hard numbers. However, a typical formal cost-benefit analysis considers the asset's value (AV), the asset's exposure factor (EF), and an event's probability of occurrence (ARO) to calculate the annualized loss expectancy (ALE) of a cybersecurity incident.

$$ALE = SLE \times EF \times AV$$

This ALE is measured pre- and post-cybersecurity controls, along with the annual cost of a safeguard (ACS), to understand the value of putting in place cybersecurity controls. If this

[13] Some publicly owned utilities can be revenue negative if taxpayers are willing to support this arrangement given their status as a monopoly, but despite this arrangement they will try to maximize revenue and minimize costs to the greatest extent permitted by law.

figure is negative, there is no monetary incentive to deploying that control, unless required to by regulations or contractual agreements. For example, if there is a 50% chance of a ransomware attack compromising 50% of data worth a total of $100,000, then cost of defense should be under $25,000 to be worthwhile.

$$Value\ of\ the\ control\ = ALE_{Pre\ control} - ALE_{post\ control} - ACS$$

Following a ransomware incident, a similar analysis occurs to ensure that company minimizes the financial impact of the event which weighs the cost of recovery by paying the ransom versus restoring the data from backups. However, if the company does not have the capability to recover from backups or the cost exceeds that of the ransom payment, business leaders will be more willing to pay the extortion rather than incur the cost of disaster recovery.

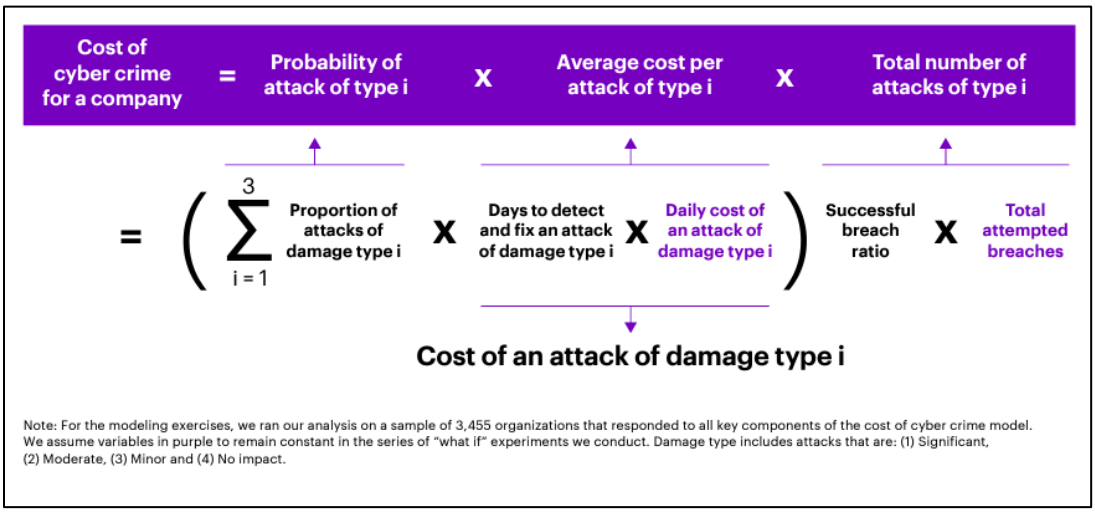

Figure 8. Formula for assessing the cost of cybercrime for a company (Accenture).

The cost of cybersecurity is too high

Unless company is a cybersecurity vender, IT security spending is typically viewed as an expense and security teams have challenges quantifying return on investment (ROI) for cybersecurity spend dollars.[cli] Cost is so important when considering risk, that "cost-effective" is mentioned throughout the gold standard risk management framework, NIST SP 800-37, and "cost-effective execution of the RMF" is listed out as a primary objective.[clii] The challenge is that cybersecurity budgets are typically a sub-percentage of larger IT budgets[cliii] and that cybersecurity technology itself is expensive, especially for smaller companies. These costs are exacerbated by the growing requirement for cybersecurity talent[cliv]— whose average salaries are increasing[clv]—to deploy and maintain these tools and create processes for an increasing amount of cybersecurity rules and regulations.[clvi]

It is difficult to quantify the total cost of cybersecurity technology for any organization as the requirements of each is different. Venders tend to not publish their prices and there are an ever-increasing number of IT providers bundling premium security into their products or shifting to service models.[clvii] Business estimates range from 6% to 20% of a company's total IT budget[clviii][clix] or on average $2,700 for full time employees in a small enterprise.[clx] Or in other words, the cost for cybersecurity is the equivalent of buying a new high-end laptop for each employee every year. This percentage can be especially difficult for small to medium companies that tend to spend their limited IT budget on a managed service provider (MSP) to also manage security. While this is estimate, the trend is that global organizations will increasingly spend their budgets on cyber cybersecurity technology and services. [clxi] Depending on the critical infrastructure industry, these cost outflows can significantly what are already slim profit margins.[clxii]

Ransomware Incident Detection and Analysis

Like cybersecurity tools used to protect networks, cybersecurity incident response is not inexpensive. If a victim chooses not to pay the ransom extortion, then victims must remove the threat actors from their network and rebuild from backups. Victims must then determine if their backups usable and up-to-date, how long it will take to restore from backups. Some ransomware variants also target backups, attempting to corrupt or delete them before a ransom note appears. [clxiii] For an example of recovery costs, incident response consulting may cost $425 per hour in a block of 740 hours, i.e., $314,500 for 31 days of incident response time.[clxiv] This coverage does not guarantee uptime following the one-month period and focuses solely on finding the threat and offering recommendations remediation. Additional costs may include the added overhead associated with employees working overtime, the need for physical travel, and the additional cost of downtime.

One victim's decision to pay a ransom marginally increases the odds of future attacks, which would marginally increase the value of defense. However, increasing odds of attack driving increased incentives to defend will almost certainly result in an unacceptably equilibrium rate of ransomware attacks on critical infrastructure without policy changes to adjust victims' and potential victims' incentives. Compare the example of one month of recovery costs for $314,500 to the average ransom payment of $211,529 or median ransom of $73,906, with an average downtime of 26 days.[clxv] Government actions that make ransom payments easier or increase the odds of having ransoms clawed back further shift victims' incentives in favor of paying ransoms. If the ransomware actor is threatening doxing, then paying a ransom also reduces the risk of lawsuits is reduced especially if there is no publicity surrounding the attack. Policies related to data breach liability from ransomware incidents must balance two goals: holding companies accountable for poor cybersecurity practices; and reducing victims' incentives to pay ransoms in order to prevent public disclosure of incidents that may lead to more costly lawsuits.

[i] E.g., "Ransomware is a critical national security threat," Portman Report; "Cyber threats to critical infrastructure represented a significant risk to the nation's economic stability," GAO report; "Ransomware is a national security priority and an area of significant concern to the U.S. government in terms of potential loss of life, financial impact, and critical infrastructure vulnerability," NMLRA 2022; DOJ giving ransomware investigations similar priority to terrorism.
[ii] AEP 2016 | Digital Blackmail As An Emerging Tactic | pg. 2
[iii] AEP 2017 | The Future of Ransomware and Social Engineering: Understanding Ransomware Trends, Users, and the Malicious Social Engineering Tactics They Use | pg. 3
[iv] Institute for Security and Technology (IST)'s Ransomware Task Force (RTF)| May 2022 | The Ransomware Task Force: One Year On
[v] FinCEN | 15 October 2021 | Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021
[vi] Staff Report for Senator Gary Peters (D-MI), Chairman, Senate Homeland Security and Governmental Affairs Committee (HSGAC) | May 2022 | Use of Cryptocurrency in Ransomware Attacks, Available Data, and National Security Concerns (hereinafter "the Peters Report") | pg. 5
[vii] AEP 2017 | Risks and Vulnerabilities of Virtual Currency: Cryptocurrency as a Payment Method | pg. 10
[viii] The Peters Report | pgs. 2, 28, 37; and footnote 98
[ix] Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 | pg. 5, Figure 2.
[x] The Ransomware Task Force: One Year On | pg. 14
[xi] Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 | pg. 5
[xii] Emsisoft Quoted in The Peters Report | pg. 2
[xiii] IST's RTF |30 April 2021 | Combating Ransomware A Comprehensive Framework for Action: Key Recommendations from the Ransomware Task Force (herein "The RTF Report")| pg. 5
[xiv] Government Accountability Office (GAO) | GAO-22-104256 | June 2022 | Cyber Insurance: Action Needed To Assess Potential Federal Response To Catastrophic Attacks |Executive summary and pg. 16.
[xv] As encouraged by the Cyberspace Solarium Commission, see, e.g., CyberScoop | 29 October 2021 | CISA starts identifying targets most necessary to protect from hacking
[xvi] The concept of a "cybersecurity poverty line" was emphasized by panelists in the RTF's Combating Ransomware: A Year of Action Reflections on the Ransomware Task Force's first year on 20 May 2022.
[xvii] The Ransomware Task Force: One Year On | pgs. 15, 18
[xviii] E.g., Workshop on the Economics of Information Security (WEIS) 2021, Yin, Sarabi, and Liu |June 2021 | Deterrence, Backup, or Insurance: A Game-Theoretic Analysis of Ransomware
[xix] Workshop on the Economics of Information Security (WEIS) 2022, Skeoch |June 2022 | Modelling Ransomware Attacks using POMDPs
[xx] U.S. DOJ | 1 July 2022 | Department of Justice Strategic Plan FYs 2022-2026 | pg. 22
[xxi] The Ransomware Task Force: One Year On | page 7
[xxii] Press release from Sen. Peters' Office| 2 June 2022 | ICYMI: Peters Releases Report on Rise of Ransomware Attacks and How Cryptocurrencies Facilitate Cybercrimes
[xxiii] DOJ | 15 July 2021 | U.S. Government Launches First One-Stop Ransomware Resource at StopRansomware.gov: New Website Provides Cybersecurity Resources from Across the Federal Government
[xxiv] E.g. Net Diligence | 15 February 2021 | Your Questions Answered about Ransomware Payments: A Q&A with Marc Grens of DigitalMint | Video beginning around 9:00
[xxv] OFAC | 21 September 2021 | Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments ("OFAC Ransomware Advisory") | pg. 5
[xxvi] The Peters Report
[xxvii] The Portman Report
[xxviii] The Peters Report | page 5, Recommendation 1.
[xxix] The Portman Report | page vi, Recommendation 3
[xxx] SEC | 9 March 2022 | Statement on Proposal for Mandatory Cybersecurity Disclosures
[xxxi] Ibid.

[xxxii] SEC | 9 March 2022 | Proposed rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure
[xxxiii] E.g., Protocol, Alspach, Kyle | 9 August 2022 | The SEC's cyberattack reporting rules are seeing fierce opposition. CISA is poised to do better.
[xxxiv] DHS Transportation Security Administration (TSA) | 20 July 2021 | DHS announces new cybersecurity requirements for critical pipeline owners and operators
[xxxv] DHS Transportation Security Administration (TSA) | 2 December 2021 | DHS Announces New Cybersecurity Requirements for Surface Transportation Owners and Operators
[xxxvi] The Peters Report | pg. 43
[xxxvii] (U) NCTC B&A n.d.
[xxxviii] The Portman Report | pg. iv
[xxxix] The RTF Report | pg. 46
[xl] The Peters Report | pg. 43
[xli] The Peters Report | pg. 40, describing CISA and FBI reporting
[xlii] The Peters Report | pg. 22
[xliii] Principal Associate Deputy Attorney General John Carlin, Head of DOJ Ransomware Task Force quoted in *Politico* | 26 April 2021 | The push for cyber funding in Biden's infrastructure plan
[xliv] E.g., Wolfram | 9 June 2021 | DarkSide Update: The FBI Hacks the Hackers?
[xlv] Eric Goldstein, Executive Assistant Director for CISA, quoted in The Peters Report | pg. 43
[xlvi] Bank Policy Institute (BPI) | 29 October 2018 | Getting to Effectiveness – Report on U.S. Financial Institution Resources Devoted to BSA/AML & Sanctions Compliance
[xlvii] The Peters Report | pg. 22
[xlviii] FinCEN | 15 June 2021 | AMLA FinCEN One Pager
[xlix] The Portman Report | pg. 15-16
[l] AEP 2017 | Risks and Vulnerabilities of Virtual Currency: Cryptocurrency as a Payment Method | pg. 10
[li] The Portman Report | pg. 15
[lii] The Guardian | 14 July 2022 | 'Lives are at stake': hacking of US hospitals highlights deadly risk of ransomware
[liii] See, e.g., The Peters Report | pg. 21 and FinCEN | FIN-2021-A004 | 8 November 2021 | Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments ("FinCEN Ransomware Advisory")
[liv] Payments identified by Wolfram | 25 May 2021 | Sleuthing DarkSide Crypto-Ransom Payments with the Wolfram Language and wallet addresses can be viewed using free tools, e.g. Blockchain.com Bitcoin Explorer
[lv] Elliptic | 7 June 2021 | US Authorities Seize the Affiliate's Share of the DarkSide Ransom Paid by Colonial Pipeline
[lvi] Some community tools, like *Etherscan.io,* label cryptocurrency wallet addresses linked to known exploits and hacks, e.g. Ronin Bridge Exploiter address,
[lvii] Treasury | 7 April 2022 | Remarks from Secretary of the Treasury Janet L. Yellen on Digital Assets
[lviii] E.g. SEC | October 2011| Investor Bulletin: The Foreign Corrupt Practices Act – Prohibition of the Payment of Bribes to Foreign Officials and
[lix] E.g. RAND Corporation, Jenkins | 2018 | Does the U.S. No-Concessions Policy Deter Kidnappings of Americans? | pgs. 9-12
[lx] Treasury | 5 April 2022 | Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex
[lxi] U.S. Department of Commerce National Institute of Standards and Technology (NIST) | NIST Special Publication 800-37 Revision 2 | December 2018 | Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy | pgs. i, ii, vi, etc.
[lxii] Motherboard Tech by Vice, Franceschi-Bicchierai, Lorenzo | 26 July 2022 | European Cops Helped 1.5 Million People Decrypt Their Ransomwared Computers
[lxiii] Wired, Greenberg, Andy | 22 August 2018 | The Untold Story of NotPetya, the Most Devastating Cyberattack in History

[lxiv] Sophos | April 2022 | The State of Ransomware 2022: Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries. | pg. 4
[lxv] The RTF Report | pg. 49
[lxvi] The RTF Report | pg. 13, 58-61
[lxvii] The National Law Review, Lazzarotti, Joseph J. | 3 January 2022 | Does Your Cyber Insurance Policy Look More Like Health Insurance?
[lxviii] Government Accountability Office (GAO) | GAO-22-104256 | June 2022 | Cyber Insurance: Action Needed To Assess Potential Federal Response To Catastrophic Attacks
[lxix] The Record by Recorded Future, Greig, Jonathan | 1 July 2022 | DOJ sets new goals for responding to ransomware attacks
[lxx] U.S. DOJ | 1 July 2022 | Department of Justice Strategic Plan FYs 2022-2026 | pg. 22
[lxxi] General Services Administration (GSA) Performance.gov | 2022 | 2YR Goal U.S. DEPARTMENT OF JUSTICE Combat Ransomware Attacks
[lxxii] FBI | n.d. | SCAMS AND SAFETY: Ransomware
[lxxiii] arXiv, Galinkin, Erick | 19 September 2021 | Winning the Ransomware Lottery? A Game-Theoretic Approach to Preventing Ransomware Attacks | pgs. 3-5
[lxxiv] Maastricht University | 2 July 2022 | Remarkable development in investigation into Maastricht University cyberattack
[lxxv] U.S. Constitution, Article I, Section 8, Clause 11
[lxxvi] U.S. Naval Institute Proceedings, Ensign Rombado, Lucian | Vol. 145/10/1,400 | October 2019 | Grant Cyber Letters of Marque to Manage "Hack Backs"; Wall Street Journal Opinion, Cyber Letters of Marque and Ransomware | 19 May 2021 | Cyber Letters of Marque and Ransomware; Cybersecurity & Information Systems Information Analysis Center (CSIAC), Colon, Frank, | Spring 2020: Volume 7 Issue 4 | Rebooting Letters of Marque for Private Sector, Active Cyber Defense; Techspective, Crowley, Jim | 12 September 2021 | Russia, China, Cyber War, and Letters of Marque and Reprisal; Los Angeles Times, Welburn, Jonathan, and Quentin Hodgson | 8 August 2021 | Op-Ed: How the U.S. can deter ransomware attacks
[lxxvii] American University, Winstead, Nicholas | 26 June 2020 | Hack-Back: Toward A Legal Framework For Cyber Self-Defense; Financial Times | 22 May 2017 | Push to let companies 'hack back' after WannaCry; and Breaking Defense, Williams, Brad | 23 July 2021 | Proposed 'Hack-Back' Bill Tells DHS To Study Allowing Companies To Retaliate
[lxxviii] U.S. Naval Institute Proceedings, Ensign Rombado, Lucian | Vol. 145/10/1,400 | October 2019 | Grant Cyber Letters of Marque to Manage "Hack Backs"
[lxxix] AFCEA International, Maclean, Don | 30 May 2018 | The Problems With Hacking Back
[lxxx] Rapid7, Ellis, Jen | 10 August 2021 | Hack Back Is Still Wack
[lxxxi] Tampa Bay Times, Mulligan, Michaela | 21 March 2022 | Canadian accused of ransomware attack on Tampa company, bitcoin worth $28M seized; The Register | 11 March 2022, Claburn, Thomas | Extradited Canadian accused of unleashing NetWalker ransomware; UNITED STATES DISTRICT COURT MIDDLE DISTRICT OF FLORIDA TAMPA DIVISION | Case 8:20-cr-00366-WFJ-SPF | UNITED STATES OF AMERICA v. SEBASTIEN VACHON-DESJARDINS Indictment; DOJ | 27 January 2021 | Department Of Justice Launches Global Action Against NetWalker Ransomware; Chainalysis | 27 January 2021 | Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware; ZDNet, Greig, Jonathan | 8 February 2022 | NetWalker ransomware gang affiliate pleads guilty and slapped with a 7-year sentence
[lxxxii] DOJ | 27 January 2021 | Department Of Justice Launches Global Action Against NetWalker Ransomware
[lxxxiii] Court Listener | Case 8:20-cr-00366-WFJ-SPF | UNITED STATES OF AMERICA v. SEBASTIEN VACHON-DESJARDINS Plea Agreement
[lxxxiv] ZDNet, Greig, Jonathan | 8 February 2022 | NetWalker ransomware gang affiliate pleads guilty and slapped with a 7-year sentence
[lxxxv] Ibid.
[lxxxvi] Chainalysis | 27 January 2021 | Chainalysis in Action: U.S. Authorities Disrupt NetWalker Ransomware
[lxxxvii] DOJ | 27 January 2021 | Department Of Justice Launches Global Action Against NetWalker Ransomware
[lxxxviii] Blockchain.com Bitcoin Explorer | Reported wallet address

[lxxxix] DOJ | 10 March 2022 | Former Canadian Government Employee Extradited to the United States to Face Charges for Dozens of Ransomware Attacks Resulting in the Payment of Tens of Millions of Dollars in Ransoms
[xc] Ibid.
[xci] ZDNet, Greig, Jonathan | 8 February 2022 | NetWalker ransomware gang affiliate pleads guilty and slapped with a 7-year sentence
[xcii] Bloomberg, Stone, Jeff | 28 June 2022 | Accused 'NetWalker' Ransomware Hacker Agrees to Plead Guilty
[xciii] BBC, Tidy, Joe | 29 June 2022 | Canadian admits to hacking spree with Russian cyber-gang
[xciv] The Record by Recorded Future, Cimpanu, Catalin | 7 February 2022 | NetWalker ransomware affiliate sentenced to seven years in prison
[xcv] DOJ | 25 March 2022 | Cybercriminal Connected to Multimillion Dollar Ransomware Attacks Sentenced for Online Fraud Schemes; Krebs on Security | 25 March 2022 | Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison; Krebs on Security | Case 1:20-cr-00145-TSE | Berezan Indictment
[xcvi] ZDNet, Tung, Liam | 10 May 2022 | Ransomware attack and COVID woes force this 150-year-old college to shut down
[xcvii] **OUTDATED** FinCEN | FIN-2020-A006 | 1 October 2020 | Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments
[xcviii] **OUTDATED** OFAC | 1 October 2020 | Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments
[xcix] FinCEN | FIN-2021-A004 | 8 November 2021 | Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments ("FinCEN Ransomware Advisory")
[c] OFAC | 21 September 2021 | Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments ("OFAC Ransomware Advisory")
[ci] Treasury's NMLRA 2022 mentions ransomware in the first paragraph of the executive summary and later states that "ransomware is a national security priority and an area of significant concern to the U.S. government in terms of potential loss of life, financial impact, and critical infrastructure vulnerability." Yet ransomware is not an NMLRA "special focus" despite prior NMLRA's hardly addressing ransomware. Further, the ransomware section in NMLRA 2022 does not describe banks' exposure to ransom-related payments or the role of professional ransom intermediaries, while overemphasizing technical aspects of cryptocurrency that are not relevant to the compliance role of most regulated FIs. Despite FinCEN's 2021 Advisory providing a description of the fiat on-ramps to ransoms, NMLRA 2022's description of the ransom payment process jumps to the cryptocurrency stage and makes no mention of DFIRs nor the MSB, SAR-filing, and sanctions compliance issues related to DFIRs. No mention is made of depository institutions' role in ransom payments. For example, the NMLRA 2022 mentions the seizure of virtual assets from a Canadian NetWalker RaaS affiliate, but does not mention that LE also seized cash and Canadian dollar-denominated bank deposits.
[cii] OFAC | 8 November 2021 | Cyber-related Designations and Designations Updates; Lursoft | n.d. | Chatextech SIA (Latvia); TRM Labs | 21 September 2021 | Behind Suex.io: the first sanctioned cryptocurrency exchange; Coindesk, Baydakova, Anna | 23 September 2021 | Binance 'De-Platforms' Russian OTC Firm Suex That Was Sanctioned by US; MTR (Estonia) | n.d. | IZIBITS OÜ
[ciii] Treasury | 21 September 2021 | Treasury Takes Robust Actions to Counter Ransomware
[civ] TRM Labs | 21 September 2021 | Behind Suex.io: the first sanctioned cryptocurrency exchange
[cv] Coindesk, Baydakova, Anna | 23 September 2021 | Binance 'De-Platforms' Russian OTC Firm Suex That Was Sanctioned by US
[cvi] OFAC | 8 November 2021 | Cyber-related Designations and Designations Updates
[cvii] Coindesk, Baydakova, Anna | 23 September 2021 | Binance 'De-Platforms' Russian OTC Firm Suex That Was Sanctioned by US
[cviii] Chainalysis | 2 February 2022 | Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class
[cix] Open-source intelligence (OSINT) on OFAC-designated wallets
[cx] Treasury | October 2021 | THE TREASURY 2021 SANCTIONS REVIEW
[cxi] https://home.treasury.gov/system/files/126/ofac_ransomware_advisory.pdf

[cxii] Treasury | 5 April 2022 | Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex; Treasury | 5 April 2022 | Russia-related Designation; Cyber-related Designation; Krebs on Security | 7 April 2022 | Actions Target Russian Govt. Botnet, Hydra Dark Market; OFAC | 8 November 2021 | Cyber-related Designations and Designations Updates; Lursoft | n.d. | Chatextech SIA (Latvia); TRM Labs | 21 September 2021 | Behind Suex.io: the first sanctioned cryptocurrency exchange; Coindesk, Baydakova, Anna | 23 September 2021 | Binance 'De-Platforms' Russian OTC Firm Suex That Was Sanctioned by US;
[cxiii] Treasury | 5 April 2022 | Treasury Sanctions Russia-Based Hydra, World's Largest Darknet Market, and Ransomware-Enabling Virtual Currency Exchange Garantex
[cxiv] Ibid.
[cxv] Ibid.
[cxvi] Bleeping Computer, Toulas, Bill | 5 April 2022 | Germany takes down Hydra, world's largest darknet market
[cxvii] Elliptic | 5 April 2022 | US Sanctions Garantex Exchange and Hydra Dark Web Marketplace Following Seizure of Hydra by German Authorities
[cxviii] DOJ | 5 April 2022 | Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace: Russian Resident Indicted on Conspiracy Charges Related to Operating Hydra Market
[cxix] DOJ | Case 22-cr-00143-CRB | 5 April 2022 | UNITED STATES OF AMERICAN v. DMITRY OLEGOVICH PAVLOV Indictment Redacted
[cxx] Elliptic | 5 April 2022 | US Sanctions Garantex Exchange and Hydra Dark Web Marketplace Following Seizure of Hydra by German Authorities
[cxxi] FBI, CISA, and Treasury | Joint Cybersecurity Advisory Alert (AA22-187A) | 6 July 2022 | North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector
[cxxii] DOJ | 19 July 2022 | Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators Two Ransom Payments Made by U.S. Health Care Providers Recovered by Law Enforcement Will Be Returned to Victims
[cxxiii] Ibid.
[cxxiv] Ibid.
[cxxv] FBI, CISA, and Treasury | Joint Cybersecurity Advisory Alert (AA22-187A) | 6 July 2022 | North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector
[cxxvi] DOJ | 19 July 2022 | Justice Department Seizes and Forfeits Approximately $500,000 from North Korean Ransomware Actors and their Conspirators Two Ransom Payments Made by U.S. Health Care Providers Recovered by Law Enforcement Will Be Returned to Victims
[cxxvii] FBI, CISA, and Treasury | Joint Cybersecurity Advisory Alert (AA22-187A) | 6 July 2022 | North Korean State-Sponsored Cyber Actors Use Maui Ransomware to Target the Healthcare and Public Health Sector
[cxxviii] The RTF Report | pg. 49
[cxxix] See, e.g., New York University Journal of Law and Business, Westbrook, Amy | Vol. 18, No. 2, 2022 | 1 December 2021 | A Safe Harbor for Ransomware Payments: Protecting Stakeholders, Hardening Targets, and Defending National Security
[cxxx] The RTF Report | pg. 50
[cxxxi] Krebs on Security | 31 May 2022 | Costa Rica May Be Pawn in Conti Ransomware Group's Bid to Rebrand, Evade Sanctions
[cxxxii] Bloomberg, Gallagher, Ryan | 27 February 2022 | Belarus Hackers Allegedly Disrupted Trains to Thwart Russia
[cxxxiii] Fast Company, Pasternack, Alex | 14 March 2022 | How hackers in Belarus are complicating Putin's Ukraine invasion
[cxxxiv] Heimdal Security, Tudor, Dora | 11 April 2022 | Conti's Leaked Ransomware Used to Target Russian Businesses
[cxxxv] FinCEN | 15 June 2021 | AMLA FinCEN One Pager
[cxxxvi] FinCEN | 10 August 2021 | FinCEN Holds Second Virtual FinCEN Exchange on Ransomware
[cxxxvii] Ibid.
[cxxxviii] Ransomware Trends in Bank Secrecy Act Data Between January 2021 and June 2021 | pg. 5, Figure 2.

[cxxxix] FinCEN | December 2021 | Illicit Finance Threat Involving Wildlife Trafficking and Related Trends in Bank Secrecy Act Data
[cxl] Deloitte | 13 September 2021 | Executives' Ransomware Concerns Are High, But Few Are Prepared for Such Attacks
[cxli] Fortinet | The 2021 Ransomware Survey Report
[cxlii] ISC2 | December 2021 | MARKET RESEARCH Ransomware in the C-Suite: An (ISC)2 Study: What Cybersecurity Leaders Need to Know About What Executives Need to Hear
[cxliii] Ibid.
[cxliv] DHS | September 2008 | A Guide to Critical Infrastructure and Key Resources Protection at the State, Regional, Local, Tribal, and Territorial Level
[cxlv] Wall Street Journal, Poulsen, Kevin, Robert McMillan, and Melanie Evans | 30 September 2021 | A Hospital Hit by Hackers, a Baby in Distress: The Case of the First Alleged Ransomware Death: NOTE: This example is given solely to demonstrate possible outcomes of ransomware attacks and is not intended to comment on the legal merits of any arguments about liability put forth in ransomware lawsuits and cases.
[cxlvi] Trend Micro Agcaoili, Janus, Miguel Ang, Earle Earnshaw, Byron Gelera, and Nikko Tamaña | 15 June 2021 | Ransomware Double Extortion and Beyond: REvil, Clop, and Conti
[cxlvii] Coveware | 3 May 2022 | Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting
[cxlviii] Kaspersky | 12 May 2022 | How Business Executives Perceive Ransomware Threat
[cxlix] OECD |2020 | Encouraging Clarity in Cyber Insurance Coverage: The Role of Public Policy and Regulation
[cl] Fitch Ratings | 15 April 2021 | Sharply Rising Cyber Insurance Claims Signal Further Risk Challenges
[cli] Forbes Technology Council, Coden, Michael | 9 May 2019 | Yes, Virginia, You Can Calculate ROI For Cybersecurity Budgets
[clii] U.S. Department of Commerce National Institute of Standards and Technology (NIST) | NIST Special Publication 800-37 Revision 2 | December 2018 | Risk Management Framework for Information Systems and Organizations A System Life Cycle Approach for Security and Privacy |pg. vi
[cliii] AT&T, Crawley, Kim | 5 May 2020 | Cybersecurity Budgets Explained: how much do companies spend on cybersecurity?
[cliv] Cybercrime Magazine, Morgan, Steve | 9 November 2021 | Cybersecurity Jobs Report: 3.5 Million Openings In 2025
[clv] Redmond, Paoli, Chris | 9 November 2021 | Report: Cybersecurity Analysts Claim Biggest Annual Salary Growth
[clvi] McKinsey, Bailey, Tucker, Justin Greis, Matt Watters, and Josh Welle | 17 June 2022 | Cybersecurity legislation: Preparing for increased reporting and transparency
[clvii] Microsoft | n.d. | Stay protected with Windows Security
[clviii] Gartner, Moore, Susan| 9 December 2016 | Gartner Says Many Organizations Falsely Equate IT Security Spending With Maturity
[clix] CSO, Violino, Bob | 20 August 2019 | How much should you spend on security?
[clx] Atlantic IT | 2022 | Cybersecurity Costs for Small Businesses
[clxi] Gartner, Moore, Susan | 17 May 2021 | Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021
[clxii] NYU, Damodaran, Aswath | January 2022 | Margins by Sector (US)
[clxiii] Threat Post | 29 September 2021 | Conti Ransomware Expands Ability to Blow Up Backups
[clxiv] State of Alaska | 30 June 2021 | Statement of work, Mandiant
[clxv] Coveware | 3 May 2022 | Ransomware Threat Actors Pivot from Big Game to Big Shame Hunting