Survey and analysis of U.S. policies to address ransomware

Jenny Blessing¹,∗, Jules Drean²,∗, and Sarah Radway³,∗

Edited by Patrick Whartenby and Kevin McDermott

HIGHLIGHTS

- There are few existing regulations and standards governing ransomware at the federal and state levels.
- Private sector self-regulation is insufficient, as organizations often lack the economic incentive and resources to maintain security standards recommended by federal agencies.
- The proliferation of ransomware is heavily enabled by cryptocurrencies. Thus, any regulation of cryptocurrency exchanges or payments will have a substantial impact on ransomware spread.

Ransomware poses a critical threat to the U.S. economy and critical infrastructure. The frequency of attacks has increased dramatically in recent years, enabled by the growing prominence of cryptocurrencies, which provide an effective means of ransom payment. In this article, we review existing policies, players, and technologies involved in the ransomware ecosystem, discussing the potential efficacy of these policies and technologies in discouraging ransomware attacks.

First, we survey the economic and technical forces driving ransomware attacks, outlining measures institutions can take to protect themselves, and summarizing the financial and political factors that motivate companies' decisions when faced with a ransomware attack. In the second half of the article, we systematize existing and pending U.S. regulatory proposals intended to mitigate the impact of ransomware, investigating: (1) blanket bans on ransomware payment, (2) mandatory reporting of ransomware incidents and payments, and (3) regulation of cryptocurrency exchange platforms. We examine the effectiveness of each of these policies as a means of preventing ransomware attacks, evaluating their impact on key players in the ransomware market.

Ransomware attacks are on the rise and show no signs of abating. Referred to as the “digital pandemic” of 2021 [1], ransomware has evolved into a thriving industry capable of threatening even the most sophisticated organizations [2]. In 2021 alone, 14 of the 16 U.S. critical infrastructure sectors, including the Defense Industrial Base, Food and Agriculture, and Emergency Services sectors, were targeted by ransomware attacks [3]. Qualitatively, ransomware incidents have had widespread impact on critical services and infrastructure in the United States and abroad. Hospitals, schools, local governments, transportation, and energy companies have all been targeted, often with disastrous effects [4, 5].

Ransomware’s growing popularity is primarily due to how lucrative these attacks can be for cybercriminals. The collective value of ransomware payments totaled at least $400 million globally in 2020, an increase of over 300% from the amount paid in 2019 [4, 6]. This number is estimated to be over $600 million for 2021, and will likely only continue to increase absent any regulatory changes [7].

However, for victims of attacks, direct financial loss is only one of several potential consequences. For businesses, loss of consumer confidence, compromised data, and general disruption to operations are possible in the aftermath of an attack, all of which directly or indirectly impact ordinary civilians. For example, in May 2021 the Colonial Pipeline Company was forced to shut down operations in response to a ransomware attack, disrupting the energy supply of much of the East Coast and leading to panic buying and widespread fuel shortages [8].

Both the public and private sectors have taken action in response to the increased frequency and severity of ransomware attacks. In this article, we summarize the technical and economic factors contributing to the rise of ransomware, and argue that even if institutions do everything “by the book”, technical solutions alone cannot prevent all ransomware attacks. We first discuss the emergence of modern ransomware, focusing on the role of cryptocurrencies and cyber-insurance. We then discuss the technical means for mitigating ransomware and their weaknesses, followed by a discussion on current policy proposals concerning ransomware, detailing the pros and cons for each policy. We then conclude with a number of key takeaways and...
has an account

Bank

Victim

Coin Exchange

Attacker

cryptocurrency's network

Figure 1: Illustration of how a ransomware payment travels from a victim’s bank account through a cryptocurrency ecosystem to the perpetrator.

considerations for policymakers.

The modern ransomware ecosystem

As defined by the U.S. Federal Bureau of Investigation (FBI), ransomware is a “type of malicious software, or malware, that prevents a victim from accessing their computer files, systems, or network infrastructure” [9]. Once a victim has been locked out, attackers demand financial payment in exchange for recovery of systems or data.

Ransomware has evolved dramatically since it was first distributed via floppy disk in 1989 [10]. Early versions of ransomware embedded the secret key, a string of random characters used for encryption and decryption, within the source code of the attack, making it easy for victims to retrieve the key and recover their files. The late 2000s saw the emergence of modern ransomware as attackers began to use more sophisticated cryptographic techniques [11]. For example, in the 2017 WannaCry attack, one of the keys required to decrypt the victim’s files is never locally stored on the victim’s machine, making it impossible to recover using classic forensic techniques [12]. Such technical measures provide a much stronger guarantee that victims will not be able to recover their data without the assistance of the attacker.

In addition, it has become more common for ransomware attacks to be carried out by diverse entities, particularly by non-technical actors who purchase malware from others, commonly referred to as Ransomware-as-a-Service (RaaS) [13]. Certain groups specialize in the ransomware development process, hiring programmers, reverse engineers, and other technically skilled workers. They then rent their services and ransom software to affiliates, usually groups with lower technical expertise, for a share of the ransom, typically around 20-25% [14]. As a result, it has never been easier for technically unsophisticated individuals to deploy ransomware.

The primary reason behind the recent rise in both the number of attacks and their effectiveness, however, is innovations in payment methods. Namely, cryptocurrencies have shifted the dynamics of the ransomware ecosystem.

Ransomware in the age of cryptocurrency

The rise of ransomware is inextricably linked to the rise of cryptocurrencies, which provide a stable, unregulated, and pseudonymous ransom payment channel and have quickly become the mechanism of choice for perpetrators [15]. Like any other industry, cybercrime is heavily shaped by underlying economic factors: without a clear revenue stream, hackers will not expend the resources to find and exploit a vulnerability.

Prior to the widespread emergence of Bitcoin and other cryptocurrencies, ransomware payments had to be made through standard banking channels which were both (1) feasible for law enforcement to trace through traditional legal methods and (2) governed by a variety of anti-money laundering and other security regulations. Financial extortionists quickly realized they could not rely on centralized, traditional payment systems like Visa or MasterCard as these entities could not only identify the attacker with relative ease but would also react to illegal activity by shutting down the payment channel used and, at times, forcibly reverting payments [16]. As a result, extortionists switched to more lenient payment systems like gift cards or premium-rate phone numbers [11]. While more reliable and effective in preserving the anonymity of the culprit, these new platforms inherently limited the amount of money that could be obtained from the victim.

Cryptocurrencies, in contrast, are largely unregulated and provide a reliable path to profitability by enabling perpetrators to demand extremely large ransoms, well beyond the transaction limits of gift cards [6]. This motivated cybercriminals to move from targeting individuals to targeting organizations, which have the financial resources and motivation to pay large ransoms [16]–[18].

In addition, cryptocurrencies are pseudonymous. While most cryptocurrency transactions are publicly viewable by anyone (in contrast to traditional banking systems), the real-world identities of the payment sender and recipient are masked, and there are a variety of technical mechanisms that can obfuscate a payment trail from one user to another (see Figure 1). In the case of ransomware, this means that the identities of perpetrators can be hard to pinpoint. Furthermore, U.S. residents are free to use cryptocurrency exchange platforms located in other countries or jurisdictions, making it challenging to apply U.S. mandates such as suspicious activity reporting or payment bans. However, as discussed later, law enforcement has been able to trace and even recover payments in certain high-profile cases.

Taken together, with the introduction of cryptocurrency

Blessing, Drean, and Radway
as a payment mechanism, the economic incentives of various actors converged: cybercriminals were given a payment channel by which they could receive much larger ransoms in a reliable manner, while the newly-targeted companies had a comparatively easy-to-use mechanism to pay the ransoms. Cryptocurrencies shifted ransomware from low-revenue, consumer-oriented attacks to a more enterprise-focused model with substantially higher revenues.

**The emergence of cyber-insurance**

The economic incentives for companies to pay ransoms have been amplified by the rapid adoption of cyber-insurance, where thousands of dollars of ransom can be covered for a reduced deductible of as little as $10,000 [19]. If it is cheaper to pay the ransom than to try to restore a system, this cost-benefit analysis will drive the insurance company’s recommendations or actions [20]. Thus, by setting ransoms to be less expensive than the estimated cost of fully restoring the system, attackers vastly increase their chances of receiving payment. While companies can decrease potential costs by maintaining frequent storage backups, in some cases the ransom will still be the cheaper and less complicated option.

Organizations frequently rely on cyber-insurance policies to finance the cost of recovery and/or ransom payments [21]. As the frequency and severity of ransomware and other cyberattacks have increased, insurers are charging higher premiums and sometimes even asking to see evidence of strong security practices and baseline network defenses. Some insurers have even gone as far as hiring outside firms with technical security expertise to vet potential clients’ security practices [21].

**Technical approaches to ransomware mitigation**

As the capabilities and frequency of ransomware attacks increase, there are extensive and evolving best practices and industry standards that organizations can take to lessen the likelihood or impact of a ransomware attack [22, 23]. We outline technical strategies surrounding ransomware incidents, examining (1) how organizations can prevent attacks, (2) how organizations can detect attacks, and (3) how organizations can recover from attacks. We examine the roles of both system administrators and system users.

**Preventative measures:** Preventative methods of mitigating ransomware attacks involve creating infrastructure and systems that are more resilient to attack.

System administrators play a large role in ransomware attack prevention [24]. When making network design choices, administrators can partition network infrastructure as damage control, limiting the flow of information between different systems to ensure that an attack does not propagate easily. When maintaining networks, system administrators should implement firewalls and monitor and address any known hardware or software vulnerabilities in their systems. In particular, it is critical that administrators ensure that software update, i.e., patches, take place regularly, so that systems are not left open to attack through known vulnerabilities.

One of the most important technical mitigation techniques is to create frequent backups of important systems and data. In the event system access is lost as part of a ransomware attack, administrators can retrieve the backup copies and recover most, if not all, compromised data [25].

System administrators can further focus on improving security threats related to human factors that have been shown to be damaging and preventable [26]. By creating user-centered systems and training personnel on everyday security threats like phishing emails [25, 26], companies can lower the likelihood of attacks. They may also go a step further and mandate various organization-wide security policies such the use of strong antivirus software, multi-factor authentication schemes, or a password manager with strong security features.

**Detection measures:** Alternatively, detection methods allow system administrators to recognize potentially malicious system access mid-attack. Administrators can monitor and investigate anomalies in network activity to detect and block traffic resembling potential ransomware attacks or traffic from known malicious IP addresses or applications [25].

Academic researchers have also proposed defense methods with the potential to invalidate common ransomware attacks [27]–[30]. For example, Mehnaz et al. [30] proposed a system that monitors file system activity in order to detect encryption from a malicious program. Their tool is able to differentiate between a normal user activity and the execution of a malware, making it possible to prevent the attack at a very early stage.

**Recovery measures:** Regardless of whether a ransom is paid, there are two components to recovery from an attack: (1) restoring systems to full functionality and (2) seeking attribution and restitution.

Regarding restoring system functionality, organizations that have implemented system backup mechanisms can largely rely on these backups after experiencing an attack. This decreases the likelihood that the ransom will need to be paid, as organizations have alternate ways of recovering their systems [25].

However, if system functionality cannot be easily restored, companies may pay the ransom. In this case, recovery efforts turn to attribution and payment recovery. Groups may attempt to trace ransomware payments with the goal of identifying the attacker and ultimately recovering the payment.

Ransomware payment is almost always demanded in cryptocurrency – typically Bitcoin – because these payment forms are largely unregulated and comparatively easy to use [6]. However, although accounts are pseudonymous, the transactions themselves are published publicly as part of Bitcoin’s decentralized audit requirement. Prior academic work has shown that it is possible to trace these financial transactions end-to-end, i.e., from the victim’s initial payment to when the cryptocurrency is converted to cash by the ransomware perpetrators, with reasonable accuracy [17, 18, 31]. Over the last half-decade, federal agencies...
have spent over $10 million in contracts with Chainalysis, a cryptocurrency-tracing firm, alone in attempts to recover payment addresses.

In several high-profile cases, law enforcement has been able to successfully identify perpetrators and recover ransom payments. For example, in June 2021, the U.S. Department of Justice (DOJ) announced it was able to recover $2.3 million of the $4.4 million that Colonial Pipeline had paid to cybercriminals the previous month [32]. DOJ’s press release revealed that it traced the payment to a specific Bitcoin address and recovered it through possession of the equivalent of the password for that particular address [32]. While it is unknown how exactly the DOJ managed to come by the password for that address, this example illustrates that, in certain cases, it is possible for law enforcement to trace and recover victim payments. This is a promising area for future academic and industrial research.

**Technical measures alone are not sufficient**

Although leveraging the technical solutions outlined above can greatly help reduce harm caused by ransomware, it is common wisdom that no system can be vulnerability-free. Zero-day exploits – vulnerabilities unknown to the software developers and users – are extremely common and have an average life expectancy of 6.9 years before discovery [33]. These zero-days can have significant consequences: in the WannaCry attack, hundreds of thousands of computers were targeted through a previously unknown vulnerability in the Windows operating system [12].

Moreover, system administrators cannot perfectly protect against human threats: users are ultimately a weak link in any system and a significant source of vulnerabilities. Using weak passwords and falling for phishing emails are examples of extremely common user behaviors that introduce insecurity into an otherwise technically sophisticated system.

Ransomware extortion cases leverage a complex business ecosystem with unexpected incentive alignments that need to be studied and addressed accordingly. For instance, even if an organization is following security best practices, there is no guarantee that it will not be in the company’s best interest to still pay the ransom. Even if a victim has put in place backup mechanisms and other methods to recover their files in the event of an attack, the cost of doing so, both in terms of time and other resources, will often outweigh the amount requested as ransom since ransom amounts are typically calculated by attackers to incentivize a victim to pay [19, 34].

As discussed previously, the current cyber-insurance market only contributes to these incentives to pay the ransom.

For these reasons and more, seeing the ransomware crisis as a purely technical problem that only calls for technical solutions is a reductive approach which is insufficient to stop the spread of ransomware attacks. To efficiently target the ransomware ecosystem, legislative tools and solutions will need to be leveraged.

**Current policies surrounding ransomware attacks and payments**

Following recent events such as the Colonial Pipeline and Brenntag attacks, U.S. policymakers have increasingly come to recognize the economic and geopolitical threats posed by ransomware. We will examine the two main approaches that are currently being explored in U.S. policy to regulate ransomware directly: (1) blanket bans on ransomware payments and (2) mandatory reporting of attacks and payments. We additionally survey regulations concerning cryptocurrency and other digital currencies given their prominence in facilitating ransomware payments. We examine and evaluate these policy approaches through key players in the ransomware ecosystem: (1) large institutions, (2) small institutions and public sector organizations, and (3) critical infrastructure. While these categorizations are not comprehensive or mutually exclusive (and in some cases overlap substantially), we believe that they capture the fundamental motivations driving ransomware policy decisions.

**Blanket bans on ransomware payments:** Given that the most common motivation behind ransomware is financial gain, some have proposed blanket bans on ransomware payments as a method of deterring cybercriminals. Under such a policy, organizations hit by ransomware would be legally prohibited from sending a ransom payment to the perpetrators and therefore unable to recover access to their systems through direct means.

While such bans represent a substantial ask of organizations hit with ransomware, they directly impact the motivation driving the ransomware ecosystem. Proponents of these bans argue that a ban on such payments would largely eliminate cybercriminals’ motivation to launch ransomware in the first place, since any ransom could not legally be paid, and the overall revenues of these criminal organizations would decrease [35].

There are also more granular options than instituting a blanket ban: a policy could take into consideration whether or not the target is critical infrastructure and ban only payments for infrastructure that is non-critical. Such a tiered policy would represent an acknowledgment of the vastly disparate security impact ransomware can have depending on its target.

**Current and proposed policies:** In November 2021, North Carolina became the first state to enact a policy banning ransomware payments when Governor Cooper signed into law a ransomware provision included in the state’s budget (1). The law effectively bans payments from “any ... entity over which the state government has oversight responsibility”, which in practice is largely comprised of state and local governments and state-funded educational institutions. At least four additional state legislatures – New York (SB S6806A, SB S6154), Pennsylvania (SB 726), Texas (HB 3892), and Florida (HB 7055) – have introduced similar legislation banning or significantly restricting ransomware payments, though none of these proposed bills have yet made it through their respective legislatures, with some dying in committee.

Most legislation restricting ransomware payments has only...
Mandatory reporting of ransomware incidents or payments: Mandatory reporting, simply put, means that an organization hit by a ransomware attack is required to provide information about the attack to the federal government. Numerous policymakers and federal agencies have pointed to the lack of data surrounding ransomware attacks as a factor in our inability to fight the ransomware epidemic on a national scale [38, 39]. Mandatory reporting is intended to provide greater insight into the ransomware environment: policymakers hope to deter future attacks through learning about current groups, targets, and models involved in the ransomware threat.

Current reporting landscape: Until recently, there was no comprehensive ransomware reporting requirement in the United States. Instead, U.S. policy consisted of limited, industry-specific regulation. Only one sector had faced mandated reporting for computer incidents: the financial sector, which has long been heavily regulated due to the potential for direct civilian harm. In 2021, financial regulators including the Federal Deposit Insurance Corporation (FDIC) and the Federal Reserve ruled that banks must inform their primary regulators within 36 hours of discovery of any incident, including ransomware attacks, that may impact the bank’s ability to function [40].

In March of 2022, however, the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) (3) was enacted as part of a larger federal appropriations bill, representing a landmark shift in federal policy. CIRCIA requires “covered entities”, i.e., most likely organizations traditionally considered to be critical infrastructure, to notify the Cybersecurity and Infrastructure Security Agency (CISA) within 72 hours of when they suffer a “cyber incident”, where cyber incident constitutes not just ransomware but a variety of different computer security attacks. CIRCIA further includes a specific ransomware provision, requiring organizations to report ransomware payments to CISA within 24 hours and specifying quality standards for these reports. While the exact definition of what constitutes a “covered entity” within critical infrastructure has not yet been determined by CISA, CIRCIA represents the most comprehensive federal legislation concerning ransomware to date.

Proposed legislation: It is clear that current U.S. ransomware reporting regulation is not comprehensive: a limited group of institutions face relatively strict standards, namely, banks under the FDIC and critical infrastructure under CIRCIA, while many other public and private sector organizations remain unaffected.

In this way, the current mandatory reporting framework functions similarly to the U.S.’s current approach to data privacy: regulation is scattered and only covers particularly vulnerable groups. For example, student data privacy is regulated by FERPA, the data privacy of children under 13 is regulated by COPPA, and federal government data privacy practices are regulated by the General Services Administration [41]. This legal structure has benefits: it allows for stronger oversight of groups with vulnerable clientele and...
greater potential impact when hit with ransomware. However, there are also inherent problems with this approach to cyber policy: it leaves behind a vast portion of private and public sector groups.

To address these concerns, broader federal legislation has been proposed in addition to CIRIAC: the Ransom Disclosure Act of 2021 (4) introduces mandatory reporting of ransomware payments for not just critical infrastructure but any public or private organization that participates in or affects interstate commerce or receives federal funds, including local governments.

**Perspectives of key players:** Incident and payment reporting proposals have generally received bilateral support among industry leaders and government [42], representing private industry’s acknowledgment that some degree of regulation is needed to tackle ransomware. Some in the private sector have been resistant to mandatory reporting legislation out of concern for the impact on their company’s reputation – U.S. officials have cited “concerns about possibly scaring off potential or existing customers, damaging their stock value, or incurring potential legal liabilities.” [43]. This fear of disclosure is a significant burden to the open sharing of information regarding current ransomware attacks and is the primary cause for resistance to reporting legislation covering a more expansive set of entities, such as the Ransom Disclosure Act.

An additional point of divergence among involved entities is the timeline under which organizations hit with ransomware would have to report the incident and/or payment, with some proposed regulations requiring reports within 24 hours of the incident while others allow for 72 hours. In general, industry has lobbied for a longer timeframe, arguing that shorter periods are overly burdensome. The version of CIRIAC that was ultimately passed, for instance, adopts a 72-hour reporting period, with industry groups testifying in support of this timeframe [42].

**Potential impact of reporting:** Mandatory reporting of ransomware is favorable for government agencies; by receiving and distributing details regarding previous attacks, governments may ensure their own systems, and other companies’ systems, will be protected. This largely stems from the wealth of information provided in reports: by examining successful malware attacks, security engineers can learn from the exhibited exploit(s), identify existing vulnerabilities that allowed the attack to occur, and resolve them to protect against future attacks. If this vulnerability needs to be addressed by an organization in the private sector, the government can direct resources towards facilitating this update, or if the vulnerability needs to be prevented on a case-by-case basis, a government agency such as CISA can add the circumstance to its best practices. As a related benefit, mandatory reporting allows for the creation of improved systems to prevent attacks: with sufficient information about vulnerabilities, researchers can create stronger defenses and test the resilience of existing anti-malware software.

Lastly, mandatory reporting permits greater ease of attribution. Through looking at large collections of malware, trends emerge in source code that can help to identify the authors – be that by looking at language or structural similarities of code, or through the use of automated tools – for example, Kaspersky’s Threat Attribution Engine [44]. Attribution is important in understanding the motivations of attackers, to predict and prevent future attacks. Most importantly, such evidence can assist law enforcement working to develop a case against cybercriminals and hold them accountable.

**Cryptocurrency regulation:** Given ransomware’s heavy dependence on cryptocurrency as a payment system, an alternative regulatory approach is to regulate the cryptocurrency ecosystem instead of regulating ransomware directly.

**Current policies:** While there are no federal laws explicitly governing cryptocurrencies, the Financial Crimes Enforcement Network (FinCEN) within the Treasury Department has determined that the 1970 Bank Secrecy Act also applies to cryptocurrencies [45]. Specifically, all “money service businesses” are within the purview of this and other anti-money laundering laws that have been around for several decades. In theory, this means that cryptocurrency exchanges and most other entities involved in cryptocurrency transactions need to comply with certain currency transaction reporting, as well as suspicious activity reporting for transactions of over $2,000 [45].

In addition to the various anti-money laundering laws, over the past few years other federal agencies have moved to set their own regulations and oversight mechanisms. The Internal Revenue Service (IRS) now considers cryptocurrency to be “property” for tax purposes, and the Securities and Exchange Commission (SEC) governs digital assets in the same manner as traditional currency.

In the United States, in the absence of federal regulation, numerous states have proposed and enacted laws governing virtual currencies. According to the National Conference of State Legislatures (NCSL), as of December 2021 seventeen states have passed laws concerning cryptocurrency and thirty-three have pending legislation [46]. Some of these regulations have focused specifically on preventing cryptocurrency’s utility as a mechanism for money laundering: for example, Missouri’s HB 1277 modified a pre-existing money laundering law to include virtual currency in its scope [46].

**Perspectives of key players:** Cryptocurrency exchange platforms have been the main subject of regulatory proposals from federal agencies, but agencies have seen varying levels of cooperation among platforms. While FinCEN officially mandates that entities providing cryptocurrency services are subject to certain reporting requirements, in practice there are numerous exchanges and brokers, including many based within the United States, that play host to lesser-known cryptocurrencies and do not comply with FinCEN regulations. These exchanges allow such illicit and often illegal activity
as their underlying revenue model depends on this business [45]. As a result, this reporting disparity causes what the SEC describes as a "huge gap in oversight", as ransomware perpetrators and victims can send and receive payments much more easily [45].

**Takeaways**

Having examined the technical and economic factors behind the proliferation of ransomware and summarized the existing policy landscape, we conclude by reviewing key takeaways and considerations for policymakers.

**Critical infrastructure**: Any proposed regulations concerning ransomware or ransomware payments should consider distinguishing between critical infrastructure and other potential targets. Certain organizations, e.g., hospitals and other healthcare entities, could potentially lead to loss of life if a ransom is not paid, suggesting different payment and/or reporting policies may be needed for such critical organizations.

**Financial trade-offs**: Proposals to ban ransomware payments should take into account the various financial trade-offs organizations hit with ransomware will face. The financial cost of rebuilding or restoring compromised systems and networks frequently far exceeds the ransom itself [19], and this calculation does not include the time and human resources that would further be expended.

**Degree of impact on ecosystem**: Mandatory reporting policies are inherently responsive, requiring organizations to take certain actions once an attack has already taken place. While such policies help to build a greater technical understanding of current ransomware techniques and exploits used, they represent an indirect deterrence against future attacks: there is an implicit assumption that the information gleaned from reports will be acted upon, and that the various actors in the ecosystem will be able to collaborate and use this knowledge to prevent future attacks.

**Role of cryptocurrencies**: The shift to cryptocurrency as the de facto ransom payment method is driving the modern ransomware market. To regulate cryptocurrency, then, is to regulate ransomware. Enforcement processes, reporting efforts, and regulatory proposals can be more effective by targeting the interdependence of cryptocurrencies and ransomware.

In summary, the ransomware industry and accompanying cryptocurrency ecosystem are constantly evolving. Any laws regulating either of them directly have been around for less than three years, so it is difficult to fully appreciate what the effects will be. Nonetheless, we argue that technical solutions alone will not be enough to prevent ransomware attacks. In the absence of a technical panacea, regulatory policy is essential to prevent ransomware from continuing to wreak havoc within the U.S. public and private sectors.

While CIRCIA (3) and other federal actions have made progress towards tackling the ransomware epidemic, incident reporting mandates are ultimately passive legislation that come into play only once an attack has already occurred. In order to substantially deter ransomware attacks, we need regulatory policy that addresses the underlying economic motivations and payment ecosystem that allow ransomware to proliferate in the first place.

**Citation**

Blessing, J., Drean, J., & Radway, S. Survey and analysis of U.S. policies to address ransomware. *MIT Science Policy Review* 3, 38-46 (2022). https://doi.org/10.38105/spr.iyuuyqypkzm.

**Open Access**

This *MIT Science Policy Review* article is licensed under a Creative Commons Attribution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this license, visit http://creativecommons.org/licenses/by/4.0/.

**Legislation cited**

(1) SB.105, 2021 Reg. Session (North Carolina 2021): North Carolina Operations Appropriations Act of 2021. https://www.ncleg.gov/Sessions/2021/Bills/Senate/PDF/S105v7.pdf.

(2) SB.S6806A, 2021 Reg Sess. (New York 2021). https://www.nysenate.gov/legislation/bills/2021/s6806.

(3) HR.2471 - 117th Congress (2021-2022): Consolidated Appropriations Act, 2022. https://www.congress.gov/bill/117th-congress/house-bill/2471/text.

(4) S.2943 - 117th Congress (2021-2022): Ransom Disclosure Act, 2021. https://www.congress.gov/117/bills/s2943/BILLS-117s2943is.pdf.

**References**

[1] Joshi, S. *The digital pandemic of ransomware attacks will continue* (The Economist, 2021). Online: https://www.economist.com/the-world-ahead/2021/11/08/the-digital-pandemic-of-ransomware-attacks-will-continue.

[2] Gartenberg, C. Apple targeted in $50 million ransomware attack resulting in unprecedented schematic leaks (2021). Online: https://www.theverge.com/2021/4/21/22396283/apple-schematics-leak-ransomware-quanta-supplier-leak.

[3] Alert (AA22-040A). Online: https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.
[4] The White House. Fact sheet: Ongoing public U.S. efforts to counter ransomware (2021). Online: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-us-efforts-to-counter-ransomware/

[5] Weiner, S. The growing threat of ransomware attacks on hospitals. American Association of Medical Colleges (2021). Online: https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals.

[6] Chainalysis. The 2021 crypto crime report Online: https://go.chainalysis.com/es/503-FAP-074/images/Chainalysis-Crypto-Crime-2021.pdf.

[7] Chainalysis. As ransomware payments continue to grow, so too does ransomware’s role in geopolitical conflict (2022). Online: https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-ransomware/.

[8] Colonial pipeline: The darkside strikes. Online: https://csrcreports.congress.gov/product/pdf/19/IN11667.

[9] Federal Bureau of Investigation. Ransomware (2020). Online: https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware.

[10] Richardson, R. & North, M. M. Ransomware: Evolution, mitigation and prevention. International Management Review 13, 10 (2017). Online: https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs.

[11] Savage, K., Coogan, P. & Lau, H. The evolution of ransomware. Symantec (2015). Online: https://docs.broadcom.com/doc/the-evolution-of-ransomware-15-en.

[12] Greenberg, A. A WannaCry flaw could help some victims get files back. Online: https://www.wired.com/2017/05/wannacry-flaw-help-windows-xp-victims-get-files-back/.

[13] Chainalysis Team. Ransomware goes mass market (2020). Online: https://blog.chainalysis.com/reports/ransomware-targets-cryptocurrency-2019/.

[14] Krebs on Security. Conti Ransomware Group Diaries (2022). URL https://krebsonsecurity.com/2022/03/conti-ransomware-group-diaries-part-i-evasion/.

[15] Perrioth, N. This is how they tell me the world ends: The cyberweapons arms race (Bloomsbury Publishing USA, 2021).

[16] O’Kane, P., Sezer, S. & Carlin, D. Evolution of ransomware. IEEE Symposium on Security and Privacy (SP) (2018).

[17] Kolodenker, E., Koch, W., Stringhini, G. & Egele, M. Paybreak: Defense against cryptographic ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 599–611 (2017). https://doi.org/10.1145/3052973.3053035.

[18] Tailor, J. P. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.

[19] Greenberg, A. A WannaCry flaw could help some victims get files back. Online: https://www.wired.com/2017/05/wannacry-flaw-help-windows-xp-victims-get-files-back/.

[20] Mehnaz, S., Mudgerikar, A. & Bertino, E. Rwguard: A real-time detection system against cryptographic ransomware. In International Symposium on Research in Attacks, Intrusions, and Defenses, 114–136 (Springer, 2018). https://10.1007/978-3-030-04819-7_10.

[21] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W. & Kirda, E. UNVEIL: A large-scale, automated approach to detecting ransomware. In 25th USENIX security symposium (USENIX security 16), 757–772 (2016). Online: https://www.usenix.org/conference/usenixsecurity16-technical-sessions/presentation/kharaz.

[22] Andronio, N., Zanero, S. & Maggi, F. Heldroid: Dissecting and detecting mobile ransomware. In International symposium on recent advances in intrusion detection, 382–404 (Springer, 2015). https://doi.org/10.1007/978-3-319-26362-3_18.

[23] Tailor, J. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.

[24] Security tip (ST19-001). Online: https://www.cisa.gov/uscert/ncas/tips/ST19-001.

[25] Wash, R. & Cooper, M. M. Who provides phishing training? Facts, stories, and people like me. In Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems, 1–12 (2018). https://doi.org/10.1145/3173574.3174066.

[26] Kolodenker, E., Koch, W., Stringhini, G. & Egele, M. Paybreak: Defense against cryptographic ransomware. In Proceedings of the 2017 ACM on Asia Conference on Computer and Communications Security, 599–611 (2017). https://doi.org/10.1145/3052973.3053035.

[27] Tailor, J. P. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.

[28] Mehnaz, S., Mudgerikar, A. & Bertino, E. Rwguard: A real-time detection system against cryptographic ransomware. In International Symposium on Research in Attacks, Intrusions, and Defenses, 114–136 (Springer, 2018). https://10.1007/978-3-030-04819-7_10.

[29] Department of Justice Office of Public Affairs. Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists darkside (2021). Online: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[30] Kharaz, A., Arshad, S., Mulliner, C., Robertson, W. & Kirda, E. UNVEIL: A large-scale, automated approach to detecting ransomware. In 25th USENIX security symposium (USENIX security 16), 757–772 (2016). Online: https://www.usenix.org/conference/usenixsecurity16-technical-sessions/presentation/kharaz.

[31] Oosthoek, K., Cable, J. & Smaragdakis, G. A tale of two markets: Investigating the ransomware payments economy (2022). Online: https://doi.org/10.48550/arxiv.2203.05298.

[32] Tailor, J. P. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.

[33] Department of Justice Office of Public Affairs. Department of Justice seizes $2.3 million in cryptocurrency paid to the ransomware extortionists darkside (2021). Online: https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

[34] Dey, D. & Lahiri, A. Should we outlaw ransomware payments? In Proceedings of the 54th Hawaii International Conference on System Sciences, 8609 (2021). Online: http://hdl.handle.net/10125/71144.

[35] Tailor, J. P. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.

[36] Tailor, J. P. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.

[37] Tailor, J. P. & Patel, A. D. A comprehensive survey: ransomware attacks prevention, monitoring and damage control. Int. J. Res. Sci. Innov 4, 116–121 (2017). Online: https://www.rsinternational.org/IRJRIssue4/116-121.pdf.
[40] Computer-security incident notification requirements for banking organizations and their bank service providers. Online: https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank.

[41] General Services Administration. Privacy Policy and Procedures Guide (2022). Online: https://www.gsa.gov/reference/gsa-privacy-program/privacy-policy-and-procedures-guide.

[42] Starks, T. & Vicens, A. The long, bumpy road to cyber incident reporting legislation — and the one still ahead (2022). Online: https://www.cyberscoop.com/incident-reporting-legislation/.

[43] Cyberattacks: Why companies keep quiet. Online: https://www.cnbc.com/id/100491610.

[44] Kaspersky threat attribution engine. Online: https://www.kaspersky.com/enterprise-security/cyber-attack-attribution-tool.

[45] United States Senate Committee on Homeland Security and Governmental Affairs. Use of cryptocurrency in ransomware attacks, available data, and national security concerns (2022). Online: https://www.hsgac.senate.gov/imo/media/doc/HSGAC%20Majority%20Cryptocurrency%20Ransomware%20Report_Executive%20Summary.pdf.

[46] National Conference of State Legislatures (NCSL). Cryptocurrency 2021 legislation (2021). Online: https://www.ncsl.org/research/financial-services-and-commerce/cryptocurrency-2021-legislation.aspx.