INSTITUTE FOR HOMELAND SECURITY

Prohibiting Government Entities from Paying Ransoms in Ransomware Attacks: A Policy Analysis

Institute for Homeland Security

Sam Houston State University

Hannah Kyle Kinney

Prohibiting Government Entities from Paying Ransoms in Ransomware Attacks: A Policy Analysis

By Hannah Kyle Kinney, J.D., M.A.

ABSTRACT

Ransomware attacks have been on the rise over the past decade and pose a substantial threat to government entities. In response to the escalating ransomware epidemic, several states have introduced legislation prohibiting government entities from paying ransoms to cybercriminals. This technical paper conducts a comprehensive analysis of such prohibitions, considering the potential economic, operational, and security implications for government organizations. This analysis begins by examining the devastating impact of ransomware attacks on government entities, including operational disruptions, the loss of critical data, and financial costs. It then evaluates the risks associated with paying ransoms, such as funding criminal enterprises and the lack of guarantee for data recovery. Additionally, the paper explores the legal landscape surrounding ransom payments by highlighting the implications of recent state laws for how government entities should respond to these attacks. Next, the paper assesses the potential benefits of enacting policies that prohibit ransom payments by government entities. These include deterring future ransomware attacks, promoting proactive cybersecurity measures, and avoiding financial contributions to criminal organizations. These benefits are weighed against the challenges and risks posed by such prohibitions, such as the potential for permanent data loss and operational disruptions in the absence of viable recovery options. This paper offers policy recommendations for lawmakers that will enable them to balance cybersecurity concerns against economic and operational considerations.

INTRODUCTION

Background on Ransomware Attacks

Ransomware is a critical national security threat worldwide which can materially affect the daily lives of all Americans. A ransomware attack involves cybercriminals deploying malicious software that encrypts critical systems and data. Following this attack, cybercriminals will demand payment often in the form of cryptocurrency such as Bitcoin for the release of the encryption. The first ransomware attack on record was in 1989 and used a floppy disk. [1] Malware on the floppy disc infected thousands of people's files, and the victims were told to send $189 to a P.O. box in Panama to restore access.[2] Ransomware attacks continued but lacked the sophistication that cryptocurrency provided, namely the ability to receive untraceable funds virtually and immediately.[3] In recent years, ransomware attacks have grown exponentially.[4] The attacks are primarily targeted at the United States which remains the top target for attempted

[1] Symantec, The Evolution of Ransomware 7 (2015).
[2] *Id.*
[3] Committee on Homeland Security and Governmental Affairs, America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies (2022).
[4] *Id.*

ransomware attacks globally as of the first half of 2024.[5][6] Ransomware has shifted from randomly targeting individuals to focusing on high-value entities, particularly government organizations.[7] Public sector entities are especially vulnerable due to commonly outdated systems, insufficient or ineffective cybersecurity measures, and the essential services they provide to critical infrastructure.

Since 2020, ransomware attacks targeting local government entities have increased dramatically. These attacks disrupt critical infrastructure services such as law enforcement, public health, and utilities. High-profile incidents like the 2018 Atlanta and 2019 Baltimore ransomware attacks are prime examples of the damage ransomware attacks can cause, leading to millions in recovery costs and significant operational downtime.[8] In addition, a 2021 Colonial Pipeline ransomware attack temporarily disrupted fuel supplies across the Eastern United States, highlighting the national security risks associated with ransomware.[9]

In response to the growing threat, many states have taken legislative action to address ransomware. Three states have passed laws prohibiting government entities from paying ransoms, which is based on the rationale that refusing payment may provide a deterrent from future attacks. These laws in Florida, North Carolina, and Tennessee emphasize the importance of fortifying public cybersecurity defenses as a proactive measure over funding criminal activities. These laws align with federal policies, including advisories from the Office of Foreign Assets Control (OFAC) and the United States Treasury Department, which restrict ransom payments to any entity linked to terrorism or violations of other sanctions.[10]

This paper examines the economic, operational, and legal implications of prohibiting ransom payments by government entities. It explores both the potential benefits of these prohibitions and the challenges they present, offering policy recommendations aimed at improving cybersecurity without undermining essential public services. The goal is to enable a balanced approach that addresses cybersecurity concerns while considering economic and operational realities.

IMPACT OF RANSOMWARE ON GOVERNMENT ENTITIES

Data Loss and Integrity Compromise

On May 7, 2019, the city of Baltimore suffered a severe ransomware attack where most of the government computer systems were infected and in which the ransomware disrupted city

---

[5] Palo Alto Ransomware Review: First Half of 2024
https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/
[6] Cyberint Ransomware Recap 2023 Report
https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report
[7] *Id.*
[8] Ransomware Taskforce, Combating Ransomware (2020)
[9] Collin Eaton and Dustin Volz, Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom. The Wall Street Journal (2021)
[10] Treasury Continues to Counter Ransomware as Part of Whole-of-Government Effort; Sanctions Ransomware Operators and Virtual Currency Exchange
https://home.treasury.gov/news/press-releases/jy0471

services.[11] The attackers demanded a ransom from Mayor Bernard "Jack" Young of approximately $76,280 in the form of Bitcoin in exchange for restoring access and not publishing stolen data.[12] Baltimore refused to pay this ransom, resulting in over $18 million in recovery costs and months of disrupted services for the parking fines database, a system used to pay water bills, property taxes and vehicle citations [13] Ultimately, the city's chief information officer stepped down over the attack.[14]

Similarly, in March of 2018, the city of Atlanta was the subject of a significant ransomware attack on city networks. This attack that shut down key municipal services, permanently deleted police dashcam footage and legal files, and ultimately affected up to six million people.[15] The attackers demanded over $50,000 in bitcoin, but the city refused to pay, leading to a prolonged recovery process that took months to restore normal services.[16] The total cost of recovery reached nearly $17 million, which included long-term system replacements.[17] The attack also exposed weaknesses in the city's cybersecurity infrastructure, which had been criticized for vulnerabilities.[18] Ransomware incidents such as the above erode public trust and emphasize the serious consequences of data breaches for government entities, such as the integrity and confidentiality of sensitive information. From an operational perspective, compromised data can hinder or prevent daily activities, delay services, and negatively impact long-term projects.

General trust from the community affected is compounded when the entities struggle to restore services like in both Baltimore and Atlanta, where systems remained disrupted for weeks. Public entities often serve vulnerable populations who rely on their services which makes the consequences of such disruptions particularly severe. Further, in many cases, the costs to the city are substantially more than the ransom demanded by the cybercriminal.

Operation Disruptions

Ransomware attacks can immediately shut down significant essential public services. In the Baltimore attack, the city's 911 dispatch system was temporarily shut down, delaying emergency response times and potentially putting people's lives at risk.[19] Ransomware incidents in other municipalities have disrupted water treatment facilities, public transportation systems, and educational institutions. [20] In Baltimore, city workers were forced to use paper-based systems, significantly delaying services while in Atlanta, the municipal court system was shut down for

[11] Niraj Chokshi, Hackers are Holding Baltimore Hostage: How They Struck and What's Next (2019)
[12] *Id.*
[13] Ransomware Taskforce, Combating Ransomware (2021)
[14] Benjamin Freed, Baltimore Ransomware Attack Was Early Attempt at Data Extortion, New Report Shows (2020) https://statescoop.com/baltimore-ransomware-crowdstrike-extortion/
[15] Kelli Young, Cyber Case Study: City of Atlanta Ransomware Incident (2021)
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] Ransomware Taskforce, Combating Ransomware (2020)
[20] *Id.*

over a week, and residents could not pay utility bills online for months.[21] These disruptions demonstrate the disaster on operational systems that ransomware attacks can cause.

Further, the aftermath of a ransomware attack can persist long after systems are restored. Recovery is often a prolonged process and requires significant financial resources to restore critical systems and sensitive data. In addition to financial recovery costs, government entities face long-term operational setbacks such as project delays, weakened cybersecurity infrastructure, and significantly decreased public trust. The attacks also reveal vulnerabilities in government systems which may further attract cybercriminals.

Financial Costs

Though some government entities have chosen to pay ransoms in order to expedite recovery, this choice presents financial and ethical challenges. Paying ransoms can impose substantial direct costs on government entities. Ransom demands from government entities can be quite high and divert funds from other critical areas. Atlanta specifically faced a ransom demand of $51,000, but the eventual recovery costs soared to an estimated $17 million.[22] Further, ransom payments, even if made, do not necessarily guarantee the return of all encrypted data. Paying the ransom additionally can encourage cybercriminals to target that entity again, or new entities.

Beyond the direct financial cost of ransom payments, the indirect costs can also be significant. These costs include expenses related to recovery efforts, potential fines for data breaches, and the increased investment required to bolster cybersecurity defenses. Baltimore's recovery expenses exceeded $18 million, which represents costs related to system upgrades, forensic investigations, and overtime pay for employees.[23]

RISKS ASSOCIATED WITH PAYING RANSOMS

Funding Criminal Enterprises

Governments paying ransom demands to cybercriminals contributes to the growth of ransomware as a lucrative business model. Cybercriminals often operate in complex networks which sometimes include “ransomware-as-a-service (RaaS), where malicious software is rented or sold to other criminals with less technical sophistication.[24] Paying ransoms directly funds these organizations, enabling them to continue their operations and invest in even more sophisticated attacks. The profitability of these attacks incentivizes further criminal activity, perpetuating a cycle of attacks. Global cybercrime damage is predicted to hit $10.5 trillion annually by 2025, driven by the financial success of these operations.[25]

There are significant ethical and legal concerns associated with paying ransoms; ethically, paying a ransom means financial supporting criminal activities and legally, if the payment is

[21] *Id.*
[22] Kelli Young, Cyber Case Study: City of Atlanta Ransomware Incident (2021)
[23] Ransomware Taskforce, Combating Ransomware (2021)
[24] *Id.*
[25] Steve Morgan, Cybercrime to Cost the World $10.5 Trillion Annually by 2025. Cybercrime Magazine (2020).

made to entities sanctioned by the government, leading to potential violations of regulations such as those enforced by the OFAC and the United States Treasury Department.

Uncertainty in Data Recovery

Even when ransom demands are paid, there is no guarantee of data recovery. In 2019, in Lake City, Florida, cybercriminals used ransomware to disable the city's computer systems.[26] The government staff worked with the FBI to attempt to restore communication systems and online utility payments but were not successful. [27] City leaders eventually called an emergency meeting and voted to pay the cybercriminals the $460,000 they demanded.[28] Unfortunately, the decryption tools provided by the cybercriminals were unreliable and caused further delays.[29] Studies have shown that paying ransoms is often an ineffective strategy.[30] Cybercriminals may fail to provide decryption tools, or the tools may only partially restore systems. A global survey conducted by Cybereason with 1,263 companies found 80 percent of victims who submitted a ransom payment experienced another attack soon after, and 46 percent got access to their data but most of it was corrupted.[31] This uncertainty underscores the risks and inefficacy of ransom payments as a recovery strategy and reinforces the need for stronger preventive measures.

Encouragement of Further Attacks

Paying ransom demands incentivizes further attacks by demonstrating the profitability of these criminal enterprises and signaling to cybercriminals that government entities are willing to capitulate. Consequently, entities that submit to ransom demands frequently become repeat targets.[32] This cycle not only drains financial resources but also degrades the overall cybersecurity posture and community trust of the affected organizations. Additionally, cybercriminals can reinvest the proceeds from successful attacks into developing more advanced methods, expanding their reach to other vulnerable entities.[33]

Moreover, ransom payments perpetuate the use of ransomware as a viable and accepted business model, which encourages its proliferation. The increasing frequency of these attacks has profound implications for the broader cybersecurity landscape. Rather than focusing on proactive security enhancements, organizations must allocate resources toward responding to attacks, weakening their long-term cyber resilience. This persistent threat landscape undermines efforts to build robust cybersecurity infrastructure.

LEGAL LANDSCAPE SURROUNDING RANSOM PAYMENTS

---

[26] Patricia Mazzei, Another Hacked Florida City Pays a Ransom, This Time for $460,000. The New York Times (2019)
[27] *Id.*
[28] *Id.*
[29] *Id.*
[30] Ransomware: The True Cost of Business, A Global Study on Ransomware Business Impact (2021) www.cybereason.com
[31] *Id.*
[32] Ransomware Taskforce, Combating Ransomware (2021)
[33] *Id.*

Overview of State Laws Prohibiting Ransom Payments

Multiple states have enacted laws prohibiting ransom payments by government entities. For example, North Carolina General Statute § 143-800 explicitly prohibits state agencies from paying ransoms and states that any state agency or local government experience a ransom request shall consult with the Department of Information Technology.[34] Florida Statute § 282.3186 mandates that state and local government entities develop strategies for responding to cyber incidents without resorting to ransom payments.[35] Many states have also introduced proposed legislation with similar aims, including Texas House Bill 3743 and Arizona House Bill 2145 which would have explicitly forbid local governments from making ransom payments to cybercriminals, emphasizing the need for alternative recovery strategies.[36] These bills have not been successful, but every year additional bills are proposed to prohibit ransomware payments from government entities.

Federal Perspectives and Guidelines

OFAC has issued advisories warning that paying ransoms to entities linked to terrorism or sanctioned countries could result in legal penalties.[37] These advisories highlight the risks of violating U.S. sanctions and emphasize the importance of reporting ransomware incidents to federal authorities. This creates a complex legal landscape, as government entities must ensure they are not inadvertently violating federal laws by making ransom payments to unknown cybercriminals.

If a government entity makes a ransom payment to a sanctioned entity, it may face significant legal consequences, including fines and sanctions.[38] This risk further incentivizes governments to avoid making payments altogether and instead invest in preventive cybersecurity measures.

There are no current Federal laws prohibiting ransomware payments, but the debate recently emerged following a memo from the Institute for Security and Technology's Ransomware Task Force.[39] The task force argues that an immediate ban could exacerbate harm to victims, society, and the economy, particularly impacting small businesses that might collapse under prolonged disruptions.[40] Currently, organizations are underprepared for ransomware attacks, especially in critical sectors like healthcare, education, and government.[41] The task force recommends a multiyear approach to reducing payments, focusing on preparedness, deterrence, disruption, and response.[42] Additionally, the task force suggests the following four step framework: Deter

---

[34] N.C.G.S. § 143-800 (2024)
[35] FL Stat § 282.3186 (2023)
[36] Benjamin Freed, Time Will Tell if States' Ransomware Payment Bans Curb Threat (2022) Https://statescoop.com/states-ransomware-payment-bans-curb-threat/
[37] Porter Wright, OFAC Updates Guidance on Ransomware Payments and Sanctions Risk (2021) https://www.technologylawsource.com/2021/09/articles/data-breach-notification/ofac-updates-guidance-on-ransomware-payments-and-sanctions-risk/
[38] *Id.*
[39] Ransomware Taskforce, Combating Ransomware (2021)
[40] *Id.*
[41] *Id.*
[42] *Id.*

Ransomware Attacks, Disrupt the Ransomware Business Model, Help Organizations Prepare, 4. Respond to Ransomware Attacks More Effectively. [43] While regulations like the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) already mandate timely reporting of ransomware incidents and payments, there is no outright ban yet.[44] Proponents of a ban argue it could decrease criminal activity, citing drops in ransomware when payments were reduced, while opponents caution that businesses might fail without recovery options and may avoid reporting attacks if payments are penalized.[45] The task force aims to revisit the feasibility of a ban once organizations can recover from attacks more effectively.[46]

Impact Of Legislation on Government Response Strategies

Government entity compliance with state laws and federal guidelines prohibiting ransom payments can be challenging. These laws necessitate the development of robust incident response plans and strong investment in cybersecurity measures to mitigate the impact of ransomware attacks without resorting to ransom payments. It requires strong coordination between legal and cybersecurity teams to ensure adherence to state law while also navigating federal guidelines. Additionally, effective coordination with federal agencies, such as the Cybersecurity and Infrastructure Security Agency (CISA) and the FBI, is crucial for government entities. These agencies provide critical resources, including technical support and intelligence sharing, to help state and local governments respond to attacks without paying ransoms.[47]

POTENTIAL BENEFITS OF PROHIBITING RANSOM PAYMENTS

Deterrence of Future Ransomware Attacks

Paying ransoms directly funds organized cybercrime, further enabling the growth of ransomware as a business.[48] By prohibiting such payments, government entities can help to cut off the financial resources that fuel these criminal enterprises. Ransomware is a financially motivated crime and if cybercriminals can no longer expect a payout from their government targets, they may seek other more lucrative alternatives. This ideally will create a strong deterrent effect which removes the economic incentives that motivate cybercriminals. Research supports this notion and shows that entities that refuse to pay ransoms are less likely to be re-targeted in future attacks.[49]

Additionally, preliminary evidence suggests that jurisdictions with strict prohibitions on ransom payments experience lower rates of ransomware attacks.[50] Several states, including North Carolina and Florida, have reported a reduction in the frequency of ransomware attacks following the enactment of legislation prohibiting ransom payments.[51] Although the deterrent

[43] *Id.*
[44] *Id.*
[45] *Id.*
[46] *Id.*
[47] *Id.*
[48] Homeland Security, Ransomware Attacks on Critical Infrastructure Sectors (2022)
[49] *Id.*
[50] *Id.*
[51] *Id.*

effect cannot be directly attributed to any single factor, these laws likely contribute to the broader trend of disincentivizing cybercriminals from targeting government entities. Furthermore, as more states enact similar legislation, attackers may increasingly shift their focus away from public sector targets and toward less regulated private entities.

Promotion of Proactive Cybersecurity Measures

As states prohibit ransomware payments by government entities, they must also focus on proactive measures. Specifically, the development of robust incident response plans which enable government entities to respond effectively to ransomware attacks, minimizing the impact and reducing the need for ransom payments.[52] When government entities are prohibited from paying ransoms, they are forced to prioritize preventive measures and incident response planning. This has led to increased investments in cybersecurity infrastructure, including stronger encryption, regular data backups, and real-time monitoring systems.[53] In addition, federal grants and funding programs such as those provided by CISA, the FBI and other federal bodies are now more widely available to support state and local governments in enhancing their cybersecurity capabilities.[54]

Prohibitions on ransom payments may encourage the development of comprehensive incident response plans. Government entities must be prepared to recover from attacks without paying a ransom, which involves creating robust data backup protocols and recovery systems. Many entities now conduct regular cybersecurity training exercises for staff and implement procedures to limit the damage that can occur during an attack.[55] These practices, driven by legislative requirements, have contributed to the overall improvement of cybersecurity resilience in the public sector.

CHALLENGES AND RISKS OF RANSOM PAYMENT PROHIBITIONS

Permanent Data Loss

One of the most significant risks associated with prohibiting ransom payments is the potential for permanent data loss. Government entities that refuse to pay ransoms may find themselves unable to recover encrypted data which can lead to prolonged service disruptions.[56] In critical sectors such as public health, law enforcement, and emergency services, the loss of sensitive data can have life-threatening consequences. This is evident in both the city of Baltimore and city of Atlanta's ransomware attacks.[57] [58]

[52] Committee on Homeland Security and Governmental Affairs, America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies (2022).
[53] *Id.*
[54] *Id.*
[55] Homeland Security, Ransomware Attacks on Critical Infrastructure Sectors (2022)
[56] Kelli Young, Cyber Case Study: City of Atlanta Ransomware Incident (2021)
[57] *Id.*
[58] Emily Stewart, Hackers Have Been Holding the City of Baltimore's Computers Hostage for 2 Weeks. Vox (2019)

Government entities are increasingly adopting strategies to mitigate the loss of sensitive data.[59] These strategies include things such as air-gapped backups, which ensure that copies of critical data are stored offline and inaccessible to ransomware attackers.[60] In addition, government entities are ensuring regular penetration testing, and vulnerability assessments to help identify weaknesses in systems before they can be exploited by cyber criminals.[61] While these strategies necessitate upfront investment, they offer a viable alternative to paying ransoms and ensure that entities can recover from attacks without paying ransoms and otherwise engaging with cybercriminals.

Investing in tough cybersecurity measures and recovery solutions is vitally important to protecting data and critical systems.[62] Government entities must explore viable recovery options and leverage federal support, utilize public-private partnerships, and adopt cutting-edge cybersecurity solutions.[63] In the cases where data is encrypted and no viable backup is available, government entities may need to rely on external assistance to recover their systems.[64] Federal agencies like CISA and the FBI offer support to state and local governments, including forensic analysis, technical assistance, and guidance on incident recovery.[65] These resources are critical in helping entities navigate the aftermath of ransomware attacks without necessarily resorting to ransom payments.

Operational Disruptions

Prohibiting ransom payments can lead to significant and catastrophic short-term operational disruptions as government entities struggle to restore their systems.[66] However, the long-term impact of refusing to pay ransoms may sometimes be less severe than initially anticipated. Entities that invest in preventive measures and recovery planning are better equipped to bounce back from attacks, minimizing long-term operational setbacks.[67] While some entities have successfully recovered from ransomware attacks without paying ransoms, others have struggled.[68] For example, the city of Atlanta spent over $2.6 million recovering from its 2018 ransomware attack, despite refusing to pay the ransom.[69] Similarly, the city of Baltimore experienced months of operational disruptions and incurred $18 million in recovery costs following their 2019 attack.[70] Neither of the cybercriminals who attacked those cities demanded a ransom anywhere close to the final amount the cities paid to recover.

---

[59] Ransomware Taskforce, Combating Ransomware (2021)
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *Id.*
[64] *Id.*
[65] *Id.*
[66] Committee on Homeland Security and Governmental Affairs, America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies (2022).
[67] *Id.*
[68] *Id.*
[69] Kelli Young, Cyber Case Study: City of Atlanta Ransomware Incident (2021)
[70] Ransomware Attack Will Cost Baltimore City $18M, Councilmember Says, CBS News https://www.cbsnews.com/baltimore/news/baltimore-city-ransomware-attack-18m/

Nevertheless, the prohibition of ransom payments may cause entities to cease reporting ransomware attacks and effectively drive them underground.[71] Additionally, if the prohibitions carve out some exceptions for specific government entities, it may cause those entities to be targeted exponentially more. [72] Cybercriminals may additionally target attacks against organizations that the government could not tolerate being disrupted or which would risk death or catastrophe.[73] These concerns highlight the challenges that government entities face when recovering from ransomware without paying and underscore the importance of strong recovery strategies and emphasizing preventative measures.

POLICY RECOMMENDATIONS

Balancing Cybersecurity Concerns and Operational Needs

Policymakers should adopt a balanced approach when crafting policies that prohibit ransom payments from government entities. A flexible framework that allows for case-by-case evaluations may be helpful to ensure that critical services are not unduly jeopardized by rigid prohibitions. Such a framework could involve collaboration between state and federal agencies, with input from cybersecurity experts, to determine the best course of action in the event of an attack. This framework should balance cybersecurity concerns with the operational needs of government entities, ensuring that the policies are both effective and practical.

To ensure an effective response to ransomware attacks, government entities must collaborate closely with federal agencies such as CISA, the FBI, and OFAC. These agencies provide vital resources, including intelligence sharing, technical support, and financial assistance for cybersecurity improvements. A coordinated effort across global, federal, state, and local levels is essential to minimizing the impact of ransomware on government entities.

Investment in Cybersecurity Infrastructure

State and local governments should prioritize adequate funding and resource allocation for cybersecurity initiatives, ensuring that they have the necessary resources to prevent and respond to ransomware attacks. Federal grants, such as those available through CISA's Cybersecurity Grant Program, can help supplement state and local funding, enabling governments to invest in advanced cybersecurity technologies and training. Ongoing training and development for government IT staff which includes regular cybersecurity training, certifications, and participation in cybersecurity exercises to enhance their skills and preparedness are vital.

Legal and Regulatory Considerations

While three states have taken steps to prohibit ransom payments, there are still many additional areas for improvement in the legislative landscape. Policymakers should consider enacting laws that provide clearer guidance on how government entities should respond to ransomware attack and update legal frameworks to address emerging cyber threats while ensuring that laws are

[71] Ransomware Tax Force, Roadmap to Potential Prohibition of Ransomware Payments (2024)
[72] *Id.*
[73] *Id.*

adaptable to evolving technologies. In addition, federal laws that address the intersection of cybersecurity and national security, such as OFAC's advisories on ransom payments, should be aligned with state-level prohibitions to create a unified legal framework.

In addition, many organizations have proposed additional reform in the form of mandating greater transparency in cryptocurrency transactions.[74] Given that the rise in frequency of ransomware attacks is directly tied to the availability of cryptocurrency, it is logical to regulate this area. Further, cryptocurrency paid in ransomware attacks has been tracked and returned.[75] This was seen in the Colonial Pipeline case, where FBI agents managed to track the ransom payment made through a Bitcoin Wallet and were able to recover nearly all of the Bitcoin paid.[76]

Current policies addressing ransomware are often insufficient in both their scope and efficacy, necessitating the introduction of more robust legislative frameworks. New legislative measures could include mandates requiring proactive cybersecurity efforts, such as incident response plans and routine system audits, especially in sectors vulnerable to attack. Additionally, laws should prioritize establishing a dedicated funding stream for cybersecurity initiatives in government entities, allowing for the adoption of advanced technologies and staff training. Further, legislation should clearly delineate protocols for ransomware response which includes timelines for reporting incidents and ensuring collaboration between state and federal cybersecurity bodies. These policies would create a more resilient infrastructure, positioning government entities to better defend against and recover from cyber threats such as ransomware attacks.

CONCLUSION

Summary of Key Findings

This paper has explored the profound impact ransomware attacks have on government entities, focusing on operational disruptions, data loss, and financial burdens. It has outlined the risks associated with paying ransoms, such as perpetuating criminal enterprises and the uncertain recovery of data. Additionally, this paper examined the legal landscape including recent state and federal legislation aimed at curbing or prohibiting ransom payments. The analysis weighed the potential benefits of prohibiting ransom payments—such as deterring future attacks and encouraging proactive cybersecurity—against the risks of operational setbacks and permanent data loss.

Final Thoughts on the Efficacy of Ransom Payment Prohibitions

Banning ransom payments by government entities offers a viable deterrence strategy against future attacks, pushing entities toward better-preparedness and cybersecurity investments. However, these prohibitions must be balanced with the practical necessity for government bodies to maintain uninterrupted operations. Without reliable recovery options in place, a strict ban may

[74] Beyond Ransomware Bans: Alternative Strategies to Address Corporate Ransomware Payments (2024) https://blogs.iu.edu/maurerglobalforum/2024/08/26/beyond-ransomware-bans-alternative-strategies-to-address-corporate-ransomware-payments/
[75] *Id.*
[76] *Id.*

lead to longer-term operational challenges. Therefore, prohibitions should be accompanied by comprehensive support systems, including clear recovery protocols and federal assistance during attacks, to ensure that the government's ability to function is not jeopardized.

Future Directions for Research and Policy Development

Future research should focus on the development of more robust and accessible recovery strategies for government entities, aiming to provide alternatives to ransom payments that allow for swift operational restoration. Policymakers should also enhance transparency regarding cryptocurrency and ensure the ability to trace ransomware payments. Additionally, cybersecurity infrastructure must be continually enhanced, with greater emphasis on training and preparedness for government staff. Policymakers should also investigate the long-term consequences of ransom payment prohibitions, examining their impact on both attack frequency and governmental resilience. Continuous policy refinement will be necessary to ensure that responses to ransomware threats evolve in tandem with the growing sophistication of cybercriminal tactics.

REFERENCES

Beyond Ransomware Bans: Alternative Strategies to Address Corporate Ransomware Payments (2024), https://blogs.iu.edu/maurerglobalforum/2024/08/26/beyond-ransomware-bans-alternative-strategies-to-address-corporate-ransomware-payments/.

Brookings Institution. (2020). *Ransomware: Federal And State Policy Responses*.

Center for Strategic and International Studies (CSIS). (2020). *Policy Approaches to Ransomware*.

Chokshi, N. (2019). Hackers Are Holding Baltimore Hostage: How They Struck and What's Next. *The New York Times*.

Committee on Homeland Security and Governmental Affairs. (2022). *America's Data Held Hostage: Case Studies in Ransomware Attacks on American Companies*.

Cyberint. (2023). *Ransomware Recap 2023 Report*. https://cyberint.com/blog/research/ransomware-trends-and-statistics-2023-report

Cybersecurity & Infrastructure Security Agency (CISA). (2021). *Ransomware Guide*.

Eaton, C., & Volz, D. (2021). Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom. *The Wall Street Journal*.

Federal Bureau of Investigation (FBI). (2020). *Ransomware Prevention and Response for CISOs*.

FL Stat. § 282.3186 (2023).

Freed, B. (2022). Time Will Tell If States' Ransomware Payment Bans Curb Threat. https://statescoop.com/states-ransomware-payment-bans-curb-threat/

H.B. 3743, 2020 Leg., Reg. Sess. (Tex. 2020).

H.B. 2145, 2022 Leg., Reg. Sess. (Ariz. 2022)

Mazzei, P. (2019). Another Hacked Florida City Pays a Ransom, This Time For $460,000. *The New York Times*.

Morgan, S. (2020). Cybercrime To Cost the World $10.5 Trillion Annually By 2025. *Cybercrime Magazine*.

N.C.G.S. § 143-800 (2024).

Palo Alto Networks. (2021). *The State of Ransomware 2021*. https://www.paloaltonetworks.com/resources/research/state-of-ransomware-2021

Palo Alto Networks. (2024). *Ransomware Review: First Half of 2024*. https://unit42.paloaltonetworks.com/unit-42-ransomware-leak-site-data-analysis/

Wright, P. (2021). OFAC Updates Guidance on Ransomware Payments and Sanctions Risk. https://www.technologylawsource.com/2021/09/articles

Ransomware: The True Cost of Business, A Global Study on Ransomware Business Impact (2021), www.cybereason.com.

Ransomware Attack Will Cost Baltimore City $18M, Councilmember Says, CBS News, https://www.cbsnews.com/baltimore/news/baltimore-city-ransomware-attack-18m/.

Ransomware Taskforce. (2020). *Combating Ransomware*.

Ransomware Task Force. (2024). *Roadmap To Potential Prohibition of Ransomware Payments*.

RAND Corporation. (2019). *Combating Cybercrime: Key Policy Issues*.

S. 7246, 2020 Leg., Reg. Sess. (N.Y. 2020).

Symantec. (2015). *The Evolution of Ransomware*.

U.S. Department of Homeland Security. (2022). *Ransomware Attacks on Critical Infrastructure Sectors*.

U.S. Department of the Treasury. (2020). *Advisory On Potential Sanctions Risks for Facilitating Ransomware Payments*.

U.S. Department of the Treasury. (2021). *Treasury Continues to Counter Ransomware As Part Of Whole-Of-Government Effort; Sanctions Ransomware Operators And Virtual Currency Exchange*. https://home.treasury.gov/news/press-releases/jy0471

Young, K. (2021). *Cyber Case Study: City Of Atlanta Ransomware Incident*.

Ransomware Taskforce. (2021). *Ransomware: The True Cost of Business, A Global Study on Ransomware Business Impact*. Cybereason. https://www.cybereason.com

AUTHOR BIOGRAPHY

Hannah Kyle Kinney, J.D., M.A., is an Associate Attorney at the De Ford Law Firm in The Woodlands, Texas. She earned her J.D. and M.A. from the University of Arizona's James E. Rogers School of Law in 2019. Subsequently, Hannah clerked for the presiding Judge at the Pima County Superior Court. Hannah is currently licensed to practice in both Arizona and Texas and specializes in domestic relations law. Her research focuses on legislative and judicial responses to issues of gender and domestic violence, contributing to a deeper understanding of these critical topics.

INSTITUTE FOR HOMELAND SECURITY

The Institute for Homeland Security at Sam Houston State University is focused on building strategic partnerships between public and private organizations through education and applied research ventures in the critical infrastructure sectors of Transportation, Energy, Chemical, Water / Wastewater, Healthcare, and Public Health.

The Institute is a center for strategic thought with the goal of contributing to the security, resilience, and business continuity of these sectors from a Texas Homeland Security perspective. This is accomplished by facilitating collaboration activities, offering education programs, and conducting research to enhance the skills of practitioners specific to natural and human caused Homeland Security events.

Institute for Homeland Security
Sam Houston State University

Kinney, H. K. (2025). Prohibiting Government Entities From Paying Ransoms in Ransomware Attacks: A Policy Analysis (Report No. IHS-2025-1002). The Sam Houston State University Institute for Homeland Security.
https://doi.org/10.17605/OSF.IO/4EX2J