

Social Implications of Ransomware Payment Ban Proposals
in the United States Healthcare System

Cristian Argint

CYSE 425W: Cybersecurity Strategy and Policy

Professor Bora Aslan

Old Dominion University

November 12, 2025

Social Implications of Ransomware Payment Ban Proposals in the United States Healthcare System

Introduction

The rise of ransomware attacks against healthcare institutions has prompted legislative discussions at the federal level regarding the potential prohibition of ransom payments. While these proposals are often framed in terms of national security and economic deterrence, the social dimensions of such a policy deserve equal attention. This paper examines the social factors that have driven the emergence of ransomware payment ban proposals, the social consequences such a policy would create, and how cultural influences have shaped the public and institutional response to ransomware threats in American healthcare.

Social Factors Driving the Policy Debate

Several social dynamics have converged to bring ransomware payment bans into the mainstream policy conversation. The first is the increasing visibility of healthcare cyberattacks in public discourse. High-profile incidents, such as the 2024 Change Healthcare breach that disrupted pharmacy operations and insurance claims processing for millions of Americans, brought cybersecurity into the everyday consciousness of people who had previously viewed it as a niche technical concern (AHA, 2024). When patients cannot fill prescriptions or access their medical records, cybersecurity becomes a social issue rather than an IT problem.

The second factor is the erosion of public trust in institutional competence. Survey data from the Pew Research Center (2024) indicates that public confidence in hospitals to protect patient data declined from 73% in 2019 to 51% in 2024. This decline reflects a broader societal trend of skepticism toward institutions, but in healthcare it carries unique weight because the relationship between patient and provider is fundamentally one of vulnerability and trust. When hospitals are perceived as unable to protect sensitive health information, it affects not only the institutions themselves but also patients' willingness to seek care and share complete medical histories.

A third driver is the growing awareness of the connection between ransom payments and organized criminal enterprises. Media coverage and government reports have emphasized that ransomware groups often operate from countries with limited law enforcement cooperation, including Russia, North Korea, and Iran (DOJ, 2024). This framing has shifted public perception from viewing ransom payments as pragmatic business decisions to viewing them as morally questionable acts that fund hostile foreign entities. The social stigma associated with paying ransoms has grown accordingly.

Social Consequences of a Payment Ban

A federal prohibition on ransomware payments would create several significant social consequences. The most immediate is the potential for healthcare access disparities to widen. Rural and safety-net hospitals, which serve disproportionately low-income and minority populations, typically have fewer cybersecurity resources than large urban medical centers (Leitner et al., 2023). A payment ban without compensatory support mechanisms could result in prolonged outages at precisely the facilities that vulnerable populations depend on most. The social equity implications are substantial: a policy intended to protect society from cybercrime could inadvertently deepen existing healthcare inequalities.

A second consequence is the potential reshaping of the healthcare workforce. Cybersecurity fatigue is already a recognized phenomenon among healthcare IT professionals, and the added pressure of operating under a payment ban, where system restoration must occur without the option of paying for decryption keys, could exacerbate burnout and attrition in an already understaffed field (HIMSS, 2024). The social dimension here is that workforce challenges in healthcare cybersecurity ultimately affect patient care quality and access.

Third, a payment ban could alter the social dynamics of incident disclosure. If paying a ransom becomes illegal, organizations that experience attacks may be incentivized to conceal incidents rather than report them, fearing legal consequences in addition to reputational damage. This would undermine the collaborative information-sharing frameworks that are essential to

collective defense in the healthcare sector. The Cyber Incident Reporting for Critical Infrastructure Act of 2022 sought to encourage transparency, but a payment ban could work at cross-purposes with these goals by creating legal risks for honest disclosure (CISA, 2023).

Cultural Influences on the Policy Debate

American cultural values play a significant role in shaping both sides of the ransomware payment debate. The cultural emphasis on individual organizational autonomy and free-market decision-making inclines many business leaders and hospital administrators to oppose government restrictions on how they respond to crises. The American Hospital Association has publicly argued against blanket bans, framing the decision to pay a ransom as one that should remain with the organization best positioned to assess the immediate risk to patient safety (AHA, 2024).

Conversely, the American cultural narrative of not negotiating with criminals or terrorists provides rhetorical support for the ban. This framing borrows from longstanding national security discourse and resonates with a public that broadly supports tough-on-crime policies. Politicians advocating for a ban have invoked this narrative effectively, positioning ransom payments as capitulation to digital extortion that undermines national resolve (Senate Committee on Homeland Security, 2024).

Cultural attitudes toward technology and privacy also influence the debate. Americans have historically been more willing than citizens of many other democracies to accept privacy trade-offs in exchange for convenience, but the healthcare context inverts this calculus. Health information is perceived as distinctly sensitive, and breaches of health data are viewed more seriously than breaches of commercial data. This cultural valuation of health privacy amplifies the social pressure on hospitals and policymakers to act decisively against ransomware, even if the specific mechanism of a payment ban is imperfect.

Conclusion

The social implications of a federal ransomware payment ban in healthcare extend well beyond the immediate technical and economic considerations. The policy debate is driven by shifting public perceptions of institutional competence, growing awareness of the global criminal ecosystem, and deeply held cultural values about autonomy, security, and the sanctity of health information. A socially responsible approach to this policy challenge must account for its differential impact on vulnerable populations, its effects on the healthcare workforce, and its potential to undermine the collaborative transparency that effective cybersecurity demands.

Moving forward, policymakers should engage directly with the communities most likely to be affected by a payment ban, invest in the cybersecurity capacity of under-resourced healthcare organizations, and create safe-harbor provisions that encourage transparency over concealment. The goal should not simply be to ban a behavior, but to reshape the social and institutional conditions that make ransomware profitable and healthcare vulnerable.

References

- American Hospital Association. (2024). *Cybersecurity and hospitals: A sector under siege*. AHA Center for Health Innovation.
- Cybersecurity and Infrastructure Security Agency. (2023). *Cyber incident reporting for critical infrastructure: Implementation guidance*. U.S. Department of Homeland Security.
- Healthcare Information and Management Systems Society. (2024). *HIMSS healthcare cybersecurity survey 2024*. HIMSS.
- Leitner, M., Pahi, T., & Skopik, F. (2023). Resilience in healthcare cybersecurity: Challenges for rural and critical access hospitals. *International Journal of Medical Informatics*, 171, 104-119.
- Pew Research Center. (2024). *Americans' trust in institutions to protect personal data*. Pew Research Center.
- Senate Committee on Homeland Security and Governmental Affairs. (2024). *Hearing on ransomware: Assessing the threat and exploring policy responses*. 118th Congress.
- U.S. Department of Justice. (2024). *Report of the Attorney General's Cyber-Digital Task Force: Ransomware and digital extortion*. DOJ.