Why Traditional Criminal Justice Deterrence Fails Against Ransomware:

An Interdisciplinary Analysis

Elliot Mason

Old Dominion University

Prof. Michael T. Cromartie

IDS 300W

March 4, 2026

Ransomware has become one of the most disruptive and financially damaging forms of cybercrime today. Hospitals have had to divert patients because they could not access medical records, local governments have paused essential public services, and private companies have lost millions of dollars after attackers encrypted their systems and demanded payment. These attacks are not rare events, they are happening more often and becoming more advanced.

Even though ransomware is illegal and carries serious criminal penalties, it continues to grow. That raises an important question: why is ransomware so difficult to deter using traditional criminal justice approaches?

Traditional criminal justice systems rely heavily on deterrence theory. The idea behind deterrence is fairly straightforward people will avoid committing crimes if the punishment is severe enough, certain enough, and swift enough to outweigh the benefits. But ransomware offenders operate in a very different environment from the one classical deterrence theory was built around. They use technology to hide their identities, operate across international borders, and often earn significant financial rewards. This paper argues that traditional deterrence fails against ransomware because it assumes identifiable offenders within enforceable legal systems, while ransomware offenders take advantage of technological anonymity and economic incentives that weaken those assumptions. By combining perspectives from criminal justice, cybersecurity, and economics, it becomes clear that ransomware persists because these systems interact in ways that reduce risk for offenders while maintaining strong rewards.

The Need for an Interdisciplinary Approach

Ransomware is not just a legal problem. It is also a technological and economic one. According to Repko and Szostak (2025), interdisciplinary research is necessary when a problem is too complex to be understood through a single discipline. That definitely applies here. Ransomware involves criminal behavior and punishment, digital infrastructure and encryption, and financial incentives and market behavior all at the same time.

If we only look at ransomware through a criminal justice lens, we focus mainly on punishment and deterrence. That helps explain how the law responds, but it does not fully explain why offenders feel protected from consequences. If we only use cybersecurity, we understand how attacks technically happen, but we miss the motivations behind them. And if we only use economics, we can explain incentives and profit, but we cannot fully address enforcement challenges. Each discipline gives part of the explanation, but none of them alone provide the full picture. That is why an interdisciplinary approach is necessary. Following Repko and Szostak's (2025) research process, this paper defines the problem, evaluates insights from each discipline, identifies conflicts, and then integrates them into a broader explanation.

Criminal Justice and the Limits of Traditional Deterrence

Deterrence theory has been central to criminal justice for decades. Gibbs (1975) explains that crime can be reduced when punishment is certain, swift, and severe. More recent research emphasizes that certainty of punishment is actually the most important factor influencing behavior (Nagin, 2013). In other words, people are less likely to commit crimes when they believe they are likely to get caught.

The issue with ransomware is that this certainty is often missing. Traditional deterrence theory developed in situations where offenders could realistically be identified and arrested within a specific legal jurisdiction. Physical crimes usually leave physical evidence, witnesses, or clear geographic boundaries. Ransomware does not work that way. Offenders use encrypted communication platforms, virtual private networks, and cryptocurrency to hide their identities. Many operate from countries that do not cooperate with U.S. law enforcement or do not prioritize cybercrime enforcement.

This drastically lowers the perceived certainty of punishment. Even though penalties for cybercrime can be severe, severity alone does not deter crime if offenders do not believe they will actually face those penalties. In ransomware cases, the gap between legal threat and actual enforcement makes deterrence less effective. The law may be strong on paper, but enforcement across borders and through digital anonymity is much more complicated in practice.

Cybersecurity: Anonymity and Structural Barriers

Cybersecurity research helps explain why identifying ransomware offenders is so difficult. Ransomware uses strong encryption to lock victims out of their systems while protecting attackers' identities. Payments are often demanded in cryptocurrency, which can obscure financial trails (Ramalho, 2018). Attackers also use anonymizing networks that make tracing their physical location extremely challenging.

In addition to technical anonymity, there are geopolitical issues. Nershi (2024) explains that some ransomware groups operate in countries where enforcement is weak or politically limited. In certain situations, governments may not prioritize stopping these actors if they mainly

target foreign victims. This creates a situation where offenders feel shielded not just by technology, but also by international politics.

From a cybersecurity perspective, ransomware is not just about individual criminal behavior. It is also about system vulnerabilities. Outdated software, weak network segmentation, and poor backup systems create opportunities for attackers. Even if law enforcement successfully arrests some individuals, the broader technological environment may still allow new offenders to enter. This shows that deterrence is not just about punishment, that it is also about reducing structural opportunities.

Economics and Incentive Structures

Economic analysis adds another important layer to this issue. Rational choice theory suggests that offenders weigh expected costs against expected benefits. In ransomware cases, the financial rewards can be very high. Brown et al. (2018) use game theory to show that attackers adjust their strategies based on how likely victims are to pay and how much protection they have. If organizations are likely to pay quickly to restore operations, attackers have more incentive to target them.

Hernandez-Castro et al. (2017) describe ransomware as an illicit market exchange. Attackers offer decryption in return for payment. As long as victims continue to pay ransoms, the market remains profitable. Cyber insurance can unintentionally contribute to this dynamic if insurance policies reimburse ransom payments, reducing long-term costs for victims while keeping attacker profits stable.

From an economic standpoint, ransomware can be a low-cost, high-reward crime. Attack tools can be reused, attacks can target multiple victims at once, and the risk of arrest is relatively low. When financial incentives are strong and perceived punishment is unlikely, traditional deterrence struggles to change behavior.

Conflicts Between Disciplinary Perspectives

There is an important tension between these disciplines. Criminal justice assumes that credible punishment influences decision-making. Cybersecurity shows that technological tools make enforcing punishment difficult. Economics suggests that offenders respond most strongly to changes in incentives.

Deterrence theory depends on the idea that punishment is realistic and enforceable. However, cybersecurity research reveals that anonymity tools and cross-border challenges weaken enforcement mechanisms. Economic models demonstrate that as long as expected profits outweigh expected costs, crime may continue regardless of legal prohibitions.

This does not mean deterrence theory is useless. Instead, it means that it needs to be adapted for cybercrime. Traditional models did not fully account for global digital networks, cryptocurrency, or transnational enforcement barriers. Without incorporating those realities, criminal justice responses may overestimate the power of legal threats alone.

Establishing Common Ground

Despite these differences, there is common ground across all three disciplines: risk. Criminal justice defines risk in terms of the likelihood of punishment. Cybersecurity defines risk

in terms of system vulnerability and traceability. Economics defines risk in terms of cost–benefit calculations.

All three perspectives agree that behavior changes when perceived risk increases relative to reward. This shared concept allows for integration. Deterrence can be reframed as depending not only on legal penalties, but also on technological traceability and economic disincentives. When these factors are considered together, deterrence becomes a broader, more realistic concept.

Integration and Comprehensive Understanding

When these insights are combined, a clearer explanation emerges. Ransomware persists because legal, technological, and economic systems interact in ways that protect offenders and maintain profitability. Weak enforcement reduces perceived legal risk. Technological anonymity strengthens that protection. High financial rewards reinforce continued offending.

These systems reinforce each other in a cycle. Low enforcement credibility increases the attractiveness of ransomware. Profits encourage further technological innovation, which improves anonymity. Improved anonymity further lowers enforcement certainty. Breaking this cycle requires action at multiple levels.

Increasing penalties alone will not be enough if offenders do not believe they will be caught. Improving cybersecurity without changing financial incentives may simply push attackers to adjust tactics. Limiting ransom payments without strengthening international cooperation may shift operations elsewhere. Effective deterrence must address legal enforcement, technological structures, and economic incentives simultaneously.

This integrated explanation reflects true interdisciplinary synthesis. Instead of treating criminal justice, cybersecurity, and economics as separate areas, it blends them into a single framework. Ransomware persists not because one discipline failed, but because multiple systems interact in ways that reduce accountability and increase reward.

Conclusion

Ransomware highlights the limitations of applying traditional deterrence theory to modern cybercrime. While deterrence emphasizes certainty and severity of punishment, ransomware offenders operate in environments where identification is difficult, enforcement is fragmented, and financial incentives are strong. Cybersecurity research shows how encryption and anonymity reduce traceability. Economic research demonstrates how profitable ransomware can be under current conditions.

An interdisciplinary approach shows that deterrence fails not because the theory itself is wrong, but because its assumptions do not fully match the digital environment. By integrating criminal justice, cybersecurity, and economics, a more complete explanation emerges. Reducing ransomware will require increasing enforcement certainty, improving technological traceability, and disrupting economic incentives at the same time. Only through coordinated, interdisciplinary strategies can deterrence become more effective in addressing cybercrime in the digital age.

References

Brown, G. D., et al. (2018). Deterrence, backup, or insurance: Game-theoretic modeling of ransomware. Journal of Cybersecurity.

Gibbs, J. P. (1975). Crime, punishment, and deterrence. Elsevier.

Hernandez-Castro, J., et al. (2017). An economic analysis of ransomware and its welfare consequences. Computers & Security, 73, 221–234.

Nagin, D. S. (2013). Deterrence in the twenty-first century. Crime and Justice, 42(1), 199–263.

Nershi, R. (2024). Informal allies: State–cybercriminal alignment in the ransomware ecosystem. International Security Review.

Ramalho, D. (2018). Ransomware: Cybercrime and cybersecurity. Journal of Cyber Policy, 3(2), 215–230.

Repko, A. F., & Szostak, R. (2025). Interdisciplinary research: Process and theory (4th ed.). SAGE Publications.