LEXARA
Journal of Law and Legal Studies
Lexara: Journal of Law and Legal Studies
Vol. 1, No. 1, 2026
E-ISSN: XXXX-XXXX
punggawajournal.com/lexara

Paying the Hacker, Funding the Ecosystem: Criminalising Ransomware Payments without Punishing Victim Organisations

H.B Hasan Basri[1]
[1] Fakultas Hukum, Universitas Islam Makassar, Indonesia
Correspondence: hbhasanbasri.dty@uim-makassar.ac.id

Article Info

Article history:

Received July 10th, 2026
Revised July 25th, 2026
Accepted July 29th, 2026

Keywords:

Criminalisation; Cyber extortion; Ransomware; Ransomware payments; Victim organisations.

ABSTRACT

Existing scholarship had explained how ransom payments sustained ransomware markets, but it had not adequately separated the systemic harm of payment from the criminal culpability of victim organisations acting under pressure. This article examined how ransomware payments could be controlled without making victim organisations the primary targets of criminal punishment. Normative legal research was conducted through statutory, conceptual, and comparative approaches using legislation, sanctions guidance, policy documents, and academic literature from Australia, the United States, and the United Kingdom. The analysis found that ransom payments maintained the profitability of Ransomware-as-a-Service and supported a wider criminal ecosystem, yet the transfer itself did not establish equal culpability in every case. Blanket criminalisation overlooked differences in knowledge, recovery capacity, threat severity, and cooperation with authorities. A victim-protective model was therefore proposed in which payments remained reportable and subject to reasonable pre-payment scrutiny, while criminal liability focused on knowing prohibited payments, concealment, false reporting, and deliberate circumvention. Limited protection for compelled reports and narrowly framed emergency exceptions preserved cooperation and proportionality. The analysis also found that state recovery support was necessary to make refusal to pay operationally realistic.

INTRODUCTION

Ransomware now operates through networks of actors who do not necessarily belong to a single group (Whelan et al., 2024). Developers may provide malware and management panels, affiliates carry out intrusions, and initial access may be purchased from brokers who have already stolen credentials or identified exploitable vulnerabilities (Reshmi, 2021). Negotiation, leak sites, and cryptocurrency proceeds can be handled by still other participants, so a victim's payment moves through a wider criminal chain. The money does not merely reward the person who issued the threat; it helps maintain the infrastructure, labour, and relationships that make repeated attacks possible. Previous payments also reveal which sectors are easier to pressure and which forms of disruption convert most readily into money. Yet the organisations supplying this money are also the parties being extorted. Payment decisions usually arise after operations have stopped, data have been stolen, or publication threats have placed management under acute pressure (Yuryna Connolly & Borrion, 2022). The transaction benefits offenders, but it does not resemble an ordinary voluntary exchange. Its economic effect on the ransomware ecosystem therefore cannot, by itself, determine the payer's criminal culpability. A hospital trying to restore clinical services is not in the same position as a company that deliberately conceals a transfer to a prohibited group. Ransomware is better understood as a digital extortion market sustained by recurring payment flows, while the legal meaning of each payment still depends on the conditions in which it is made.

States have not agreed on the proper object of regulation (Teichmann, 2026). Australia emphasises reporting after payment. The United States relies more heavily on sanctions directed at particular recipients. The United Kingdom is developing a more limited prohibition for public bodies and critical infrastructure, accompanied by government engagement before payment. These approaches do not regulate the same conduct or pursue their objectives in the same way. Some focus on the payer, others on the recipient, while reporting and pre-payment scrutiny provide alternative entry points. The disagreement shows that the issue is not exhausted by asking whether a ransom may be paid. The identity of the recipient, the type of organisation, the nature of the threat, and the openness of the transaction all alter its legal meaning.

Academic debate is still often confined to a narrow choice between allowing victims to pay and banning payment altogether. The case for restriction is substantial because ransomware remains attractive while offenders continue to obtain revenue. A general prohibition, however, overlooks differences in victims' ability to recover (Matthijsse et al., 2025). A large organisation with segregated backups may be able to refuse a demand, while a small hospital or local authority may face disruption that immediately affects third parties (Mott et al., 2024). The ransom amount does not capture delayed services, recovery costs, or damaged trust. Scholarship has examined the economics of payment and the regulatory instruments available to constrain it, but it has not sufficiently explained when a payment made under pressure becomes conduct deserving criminal punishment (Worsley et al., 2025). An emergency payment intended to preserve an essential service is still too often placed in the same analytical category as a transaction deliberately concealed through an intermediary. Differences in knowledge, the severity of the threat, and the organisation's engagement with public authorities are not consistently used to differentiate sanctions. As a result, a victim's contribution to the continuation of an illegal market is sometimes treated as if it were equivalent to criminal participation, even though the relationship is far less direct.

This article examines ransomware payment as both a source of income for an extortion market and a decision made by a victim under pressure. It asks how law can reduce payment flows without converting victim organisations into the primary objects of punishment. The analysis distinguishes ordinary payment from transfers to known prohibited recipients and treats emergency conditions, concealment, and engagement with authorities as factors that alter the legal assessment. The article argues that payment should remain subject to control but should not be criminalised merely because a transfer occurred. Criminal law is better directed at knowing prohibited payments, false information, deliberate concealment, and the use of intermediaries to evade oversight. Organisations that report promptly and act to prevent serious harm require limited protection. The model developed below combines protected reporting with reasonable pre-payment scrutiny, a narrow emergency exception, and responsibility for facilitators who knowingly assist circumvention, while recognising that state recovery support affects whether refusal to pay is realistic.

RESEARCH METHODS

This article uses normative legal research supported by statutory, conceptual, and comparative approaches (Negara, 2023; Taekema, 2021). The statutory approach examines rules concerning ransomware payments, incident reporting, sanctions, and protections available to victim organisations. The conceptual approach considers the relationship between victim status, criminal culpability, proportionality, and the protection of third parties. The comparative approach identifies differences in regulation in Australia, the United States, and the United Kingdom. It is confined to rules and policies that directly concern ransomware payments and does not attempt to compare the legal systems of those jurisdictions as a whole.

Materials were collected through library and document research using official government websites, legislation databases, and open academic sources. They include legislation, sanctions advisories, official guidance, government consultation documents, institutional reports, and academic studies on Ransomware-as-a-Service, ransom payments, and the position of victim organisations. Materials were selected purposively according to their direct relevance, identifiable provenance, and availability in full text. The materials are analysed qualitatively by interpreting relevant rules and comparing the regulatory patterns found in each jurisdiction. Attention is directed to the scope of restrictions, reporting duties, protection of information, emergency conditions, and available sanctions.

RESULTS AND DISCUSSION

1. Ransomware Payments as Financing the Criminal Ecosystem

The Ransomware-as-a-Service model means that an attack no longer has to be conducted by one group controlling every stage of the process (Saccone et al., 2025). Developers may supply malware and management panels, affiliates conduct intrusions, and initial network access may be purchased from actors who have already compromised a target. Once payment occurs, proceeds are divided according to the participants' roles and agreements. Funds paid by the victim therefore sustain more than the person who issued the threat; they support working relationships and capabilities that can be reused even when one group is disrupted (Oosthoek et al., 2023). Ransom money also covers costs that are less visible from outside. Infrastructure must be maintained, malware updated, and affiliates kept interested in a profitable service. Research into the Conti group shows that ransomware operations can involve divisions of labour, recurring payments, and internal expenditure (Ruellan et al., 2024). The finding should not be generalised to every group, but it demonstrates that sustained campaigns require coordination and resources. Continued victim payments therefore help preserve technical capacity and make service-based offending attractive to actors who cannot develop their own malware, even where the use of each part of the proceeds cannot be traced.

Payment data still contain a large dark area. Cryptocurrency addresses can change, victims do not always report, and the attribution of a wallet to a particular group may be revised when new information emerges. Open datasets are useful in showing that payment flows are substantial and recurrent, but they cannot measure the entire market with certainty. Visible amounts are better treated as a lower bound than as a complete account of criminal revenue. Some transactions may be conducted through intermediaries, moved into other assets, or sent to addresses that have not yet been identified. A decline in detected transactions therefore does not automatically establish that payments or attacks have actually fallen (Meurs et al., 2026; Turner et al., 2020).

Reputation has economic value in a market without enforceable contracts. Victims may be less willing to pay a group known for defective decryptors or for publishing data after receiving money. Offenders can still break their promises, and many victims do not recover fully, but a group that repeatedly fails to honour an arrangement can damage its own prospects of obtaining later payments. Group names, victims' experiences, and information circulating among negotiators create a fragile measure of trust, so threats and promises must remain sufficiently plausible to enter the victim's decision under time pressure (Georgiou et al., 2026). Payments also provide information that can influence later demands. The cost of disruption, recovery capacity, revenue, insurance, or dependence on a particular system may shape the amount demanded and the form of pressure used, although offenders can misjudge these factors. Successful transactions may therefore refine target selection and contribute, in a limited sense, to price formation in an illegal market (Hernandez-Castro et al., 2020). This does not prove that one payment causes a later attack. It explains why the consequences of payment can extend beyond the immediate incident by preserving expectations about which targets remain profitable.

For an organisation under attack, payment may still appear rational (Vakhitova & Mezzetti, 2026). Backups may be damaged or unavailable, important data may have been taken, and disruption costs continue to grow. The difficulty arises because a choice that reduces one victim's loss can preserve offender revenue at the collective level. A payment made in good faith can therefore strengthen economic incentives without making the victim morally equivalent to the offender. Victims face threats deliberately designed to narrow their options, and the capacity to refuse is unevenly distributed. A large organisation may have segregated backups, an incident-response team, and sufficient recovery funds, while smaller public bodies can face a narrower range of options (Marett & Nabors, 2021). The consequences are particularly serious where essential services are involved; hospital ransomware can impose costs on patients and others who played no part in the organisation's security decisions (Neprash et al., 2024). A uniform prohibition may therefore impose very different burdens. Collective security can justify regulation, but the proportionality of that regulation depends on whether the organisation could realistically recover without paying and on who bears the cost when services remain unavailable.

2. Limits of Criminalisation and the Risk of Punishing Victim Organisations

A prohibition based only on the existence of payment would equate situations that are materially different. A hospital attempting to restore clinical systems does not occupy the same position as a company that knows the recipient appears on a sanctions list and nevertheless arranges the transfer

through another party. Both send money to ransomware offenders, but the pressure they face, the information available, and the way the decision is implemented differ. Criminal liability must therefore examine the fault accompanying the decision, including who within the organisation knew of the restriction and who had authority to approve payment. Pressure generated by ransomware will not always satisfy the requirements of a duress defence. Threats to reputation or commercial loss may not carry the same weight as the suspension of medical services or a danger to human safety (Corbet & Goodell, 2022). Even where pressure does not excuse liability, it remains relevant to the assessment of fault. Decision-makers may confront disabled systems, unusable backups, incomplete information, and conflicting advice. Their conduct should be assessed from the information reasonably available when the decision was taken, not solely from knowledge acquired after the crisis. A failed payment does not automatically prove recklessness, just as obtaining a working decryptor does not make the transfer lawful. The relevant inquiry is whether the organisation genuinely examined available options, sought assistance, and considered foreseeable harm before paying.

The instruments compared in this article do not have the same legal status. Australia has enacted a payment-reporting duty for specified entities, the United States primarily controls transactions through sanctions, and the United Kingdom is still developing a limited prohibition for public bodies and critical infrastructure (Cyber Security Act 2024 (Cth); Home Office, 2025a, 2025b; U.S. Department of the Treasury, 2021). An administrative advisory, binding legislation, and a government proposal cannot be read as if they carry the same legal force. What can be compared is how they constrain payment decisions. The United States sanctions regime also shows why the recipient cannot be separated from the legal assessment. OFAC may impose civil liability even where the payer did not know that a transaction involved a sanctioned person, while cooperation and compliance measures can influence enforcement. That strict civil model should not be transferred automatically into criminal law. General awareness that ransom money benefits offenders differs from knowledge that the particular recipient is prohibited. More serious criminal fault should require more concrete knowledge, or at least a clear disregard of credible information about the recipient after it has been brought to the organisation's attention.

Reporting creates a different tension. Governments need payment information and destination addresses to trace funds and connect incidents, while organisations may hesitate to provide a full account if the report immediately exposes them to additional legal consequences. Australia addresses part of this problem by limiting the use and further disclosure of information contained in mandatory reports, without preventing authorities from using evidence obtained independently. The purpose is to stop compelled cooperation from becoming the sole basis for additional disadvantage to a victim that is still recovering (Murray et al., 2025; Cyber Security Act 2024 (Cth)). The proportionality problem becomes sharper when disruption affects third parties. When a hospital cannot restore systems promptly, patients and clinical staff can bear direct consequences (Neprash et al., 2026; Vinogradskiy et al., 2024). The United Kingdom's proposals target public bodies and critical infrastructure precisely because of the importance of those services, although the measures remain under development rather than evidence of a model already proven to succeed (Home Office, 2025a, 2025b). A payment rule should therefore consider not only the interest in cutting offender revenue but also the harm caused by prolonged disruption of essential services.

An excessively broad prohibition may also make payment more difficult for authorities to discover. An organisation may hand the process to an insurer or incident-response consultant, so the formal transfer is no longer made by the direct victim (Cartwright et al., 2023). This possibility does not establish that concealment occurs in every case, but it shows why law should focus on the conduct surrounding the transaction rather than only on the person who executes it. Deliberate false information, concealment of the recipient, or continuation after a known restriction carries a different degree of fault from an incomplete or delayed report during an unfolding incident. Administrative shortcomings can be addressed through proportionate non-criminal measures, while deliberate concealment or conscious circumvention provides a stronger basis for criminal punishment. This distinction preserves incentives to report candidly because treating every reporting error as criminal may reduce the quality and timeliness of information reaching the state (Busetti & Scanni, 2025). It also prevents victim status from becoming immunity. Victim-offender inversion arises when payment itself becomes the basis of criminalisation without sufficient attention to pressure, knowledge, and post-incident conduct; it does not describe every reporting duty or administrative fine (Luu et al., 2025).

3. Victim-Protective Control of Ransomware Payments

Ransomware payment should not become a criminal offence merely because funds were ultimately transferred. The default rule proposed here is narrower: payment remains subject to oversight and reporting, while a more serious response is reserved for transfers involving recipients whose prohibited status is known. The organisation's conduct determines the level of responsibility. A delay that can still be explained differs from a decision to conceal the recipient or evade a restriction after the legal risk has become clear (Bhatt et al., 2025). This principle matters most when the attacker's identity cannot be confirmed. The United States sanctions regime shows that a payment may be prohibited because it involves a listed person, but its strict civil consequences do not justify criminalising every attribution error. Recipient checks should therefore be used to assess reasonable care rather than require a victim to perform technical attribution that may only be possible for the state. Where credible information suggests a sanctions connection, the organisation should seek available guidance and record the reasons for its decision. Criminal fault becomes stronger where the restriction is known, or the risk has been explained with sufficient clarity, and the payment is nevertheless routed through another party to conceal it. The basis for punishment lies in that knowledge and evasion, not in the victim's inability to identify an offender under severe time pressure (U.S. Department of the Treasury, 2021).

Public authorities have limited information of their own. Pre-payment notice may create an opportunity to check the recipient, connect the incident with another investigation, or identify an available recovery tool (Oz et al., 2022). The United Kingdom is developing a mechanism of this kind alongside a targeted approach for public bodies and critical infrastructure, but it has not become a general payment ban. Notice therefore cannot be assumed to produce a timely answer in every case, and honest disclosure should matter when authorities cannot provide clarity within the required period (Home Office, 2025a, 2025b). Post-payment reporting remains essential for the same reason. Australia requires covered entities to report information that is known or can be identified through a reasonable search and limits the use and further disclosure of reports. The model proposed here follows that logic: compelled information should not, by itself, construct criminal fault, although independently obtained evidence remains usable and protection ends where the organisation lies or conceals the transaction (Cyber Security Act 2024 (Cth)).

A prohibition is hardest to apply where refusing payment could prolong disruption that endangers people or disables an essential service. The exception should not extend to every commercial loss. It is justified only where there is a direct and serious risk and no alternative recovery path can operate within the required time. In an urgent case the decision may have to be taken first and reviewed once the situation is under control. The review should not depend on whether decryption succeeded. It should examine the reasons available at the time, the honesty of information supplied to the authorities, and the seriousness with which alternatives were considered. The state's responsibility also matters here. Payment restrictions are more proportionate when government provides technical support, shares available information about the recipient, and assists recovery for organisations delivering essential services. It reduces the risk that the state prohibits payment while shifting the cost of disruption to patients, residents, or service users (Hansel & Silomon, 2024; Home Office, 2025a; Welburn & Strong, 2022).

The victim does not always execute the payment (Teichmann & Wittmann, 2023). Insurers, incident-response companies, law firms, or financial service providers may influence or implement the transaction. Professional status is not the basis of liability; control over the payment and knowledge of the restriction are more important. OFAC already warns that companies facilitating payment may face sanctions exposure. Under the model proposed here, an intermediary should face criminal liability only where it knows of a restriction and uses its role to disguise the recipient or evade the applicable duty (U.S. Department of the Treasury, 2021). Within the victim organisation, knowledge should likewise be connected to a person with real authority to approve payment rather than automatically attributed from information held by technical staff. The resulting model is straightforward. Payment is not criminalised generally, reporting remains compulsory for covered organisations, and serious sanctions attach to knowing prohibited payments, false statements, deliberate concealment, and conscious circumvention. A narrow emergency exception remains available where serious harm cannot be prevented quickly by another means. The model's central distinction is between openness and culpability: limited knowledge and honest engagement weaken the case for punishment, while deliberate obscuring of a known legal risk strengthens it.

CONCLUSION

Ransomware payments strengthen the economic continuity of the extortion market because victims' funds keep offender operations profitable and create room for further attacks. That effect is not sufficient to treat every paying organisation as a criminal participant. Payment decisions are made under pressure, with incomplete information and unequal recovery capacity. Law cannot therefore evaluate every transaction solely from the fact that funds were transferred. Culpability becomes clearer where the organisation knows that the recipient is prohibited and nevertheless conceals the transaction, supplies false information, or uses another party to evade oversight. An organisation that reports promptly, attempts to check the recipient, and acts to prevent serious harm occupies a different position. A blanket prohibition is consequently inconsistent with culpability and proportionality, while also risking additional harm to victims and to people who depend on their services.

A more appropriate system does not rely on the general criminalisation of payment. Transactions remain subject to reporting, reasonable pre-payment scrutiny, and restrictions directed at recipients known to be prohibited. Information that must be reported receives limited protection so that a victim's openness does not itself become the source of a new sanction, without preventing the use of evidence obtained independently. Emergency conditions must also be considered where refusal creates a direct risk to people or essential services. Criminal law is then directed at conduct displaying more serious fault, particularly concealment, false statements, and deliberate circumvention. The state must simultaneously strengthen recovery support so that organisations have a realistic opportunity to refuse a demand. This structure allows law to constrain ransomware financing without erasing the legal position of the organisation as a victim.

REFERENCES

Bhatt, P., Valecha, R., & Rao, H. R. (2025). Situational awareness about data breaches and ransomware attacks: A multi-dimensional cyber threat impact framework and content analyses of practitioner-public discourses. *International Journal of Information Management, 83*, 102902. https://doi.org/10.1016/j.ijinfomgt.2025.102902

Busetti, S., & Scanni, F. M. (2025). Evaluating incident reporting in cybersecurity: From threat detection to policy learning. *Government Information Quarterly, 42*(1), 102000. https://doi.org/10.1016/j.giq.2024.102000

Cartwright, A., Cartwright, E., MacColl, J., Mott, G., Turner, S., Sullivan, J., & Nurse, J. R. C. (2023). How cyber insurance influences the ransomware payment decision: Theory and evidence. *The Geneva Papers on Risk and Insurance—Issues and Practice, 48*(2), 300–331. https://doi.org/10.1057/s41288-023-00288-8

Corbet, S., & Goodell, J. W. (2022). The reputational contagion effects of ransomware attacks. *Finance Research Letters, 47*, 102715. https://doi.org/10.1016/j.frl.2022.102715

Cyber Security Act 2024 (Cth) (Australia).

Georgiou, M., Giebels, E., Oostinga, M. S. D., & Spithoven, R. (2026). Engaging with cybercriminals: Phases and influence strategies in ransomware negotiations. *Computers in Human Behavior, 181*, 108953. https://doi.org/10.1016/j.chb.2026.108953

Hansel, M., & Silomon, J. (2024). Ransomware as a threat to peace and security: Understanding and avoiding political worst-case scenarios. *Journal of Cyber Policy, 9*(2), 159–178. https://doi.org/10.1080/23738871.2024.2357092

Hernandez-Castro, J., Cartwright, A., & Cartwright, E. (2020). An economic analysis of ransomware and its welfare consequences. *Royal Society Open Science, 7*(3), 190023. https://doi.org/10.1098/rsos.190023

Home Office. (2025a). Ransomware legislative proposals: Reducing payments to cyber criminals and increasing incident reporting. UK Government. https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/ransomware-legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

Home Office. (2025b). Government response to ransomware legislative proposals: Reducing payments to cyber criminals and increasing incident reporting. UK Government. https://www.gov.uk/government/consultations/ransomware-proposals-to-increase-incident-reporting-and-reduce-payments-to-criminals/outcome/government-response-to-ransomware-

legislative-proposals-reducing-payments-to-cyber-criminals-and-increasing-incident-reporting-accessible

Kadir, Z. K. (2024). Dari Dualisme ke Monisme: Transformasi Konsep Mens Rea dalam Kodifikasi KUHP di Negara-Negara Poskolonial. *Jurnal Litigasi Amsir*, (Special Issue), 142–155.

Kadir, Z. K. (2025). Kejahatan Berbasis Identitas Digital: Menggagas Kebijakan Kriminal untuk Dunia Metaverse. *Jurnal Litigasi Amsir*, *12*(2), 124–137.

Kadir, Z. K. (2026). Preventing Murder Without Expanding Punishment: Rethinking Homicide Policy Beyond Deterrence. *Punggawa Law Review*, *1*(3), 49–58. https://doi.org/10.67707/plr.v1i3.40

Luu, T. J., Samuel, B. M., Jones, M., & Barnes, J. C. (2025). Exploring how the Dark Triad shapes cybercrime responses. *Personality and Individual Differences, 244*, 113250. https://doi.org/10.1016/j.paid.2025.113250

Marett, K., & Nabors, M. (2021). Local learning from municipal ransomware attacks: A geographically weighted analysis. *Information & Management, 58*(7), 103482. https://doi.org/10.1016/j.im.2021.103482

Matthijsse, S. R., Moneva, A., van 't Hoff-de Goede, M. S., & Leukfeldt, E. R. (2025). Examining ransomware payment decision-making among small- and medium-sized enterprises. *European Journal of Criminology, 22*(4), 625–645. https://doi.org/10.1177/14773708241285671

Meurs, T., Junger, M., Cruyff, M., & van der Heijden, P. G. M. (2026). Estimating the number of ransomware attacks. *Journal of Quantitative Criminology, 42*, 227–243. https://doi.org/10.1007/s10940-025-09625-7

Mott, G., Turner, S., Nurse, J. R. C., Pattnaik, N., MacColl, J., Huesch, P., & Sullivan, J. (2024). "There was a bit of PTSD every time I walked through the office door": Ransomware harms and the factors that influence the victim organisation's experience. *Journal of Cybersecurity, 10*(1), tyae013. https://doi.org/10.1093/cybsec/tyae013

Murray, G., Falkeling, M., & Gao, S. (2025). Trends and challenges in research into the human aspects of ransomware: A systematic mapping study. *Information and Computer Security, 33*(2), 161–195. https://doi.org/10.1108/ICS-12-2022-0195

Negara, T. A. S. (2023). Normative legal research in Indonesia: Its origins and approaches. *Audito Comparative Law Journal, 4*(1), 1–9. https://doi.org/10.22219/aclj.v4i1.24855

Neprash, H. T., McGlave, C. C., Rydberg, K., & Henning-Smith, C. (2024). What happens to rural hospitals during a ransomware attack? Evidence from Medicare data. *The Journal of Rural Health, 40*(4), 728–737. https://doi.org/10.1111/jrh.12834

Neprash, H., McGlave, C., & Nikpay, S. (2026). Hacked to pieces? The effects of ransomware attacks on hospitals and patients. *American Economic Journal: Economic Policy, 18*(1), 256–281. https://doi.org/10.1257/pol.20240594

Oosthoek, K., Cable, J., & Smaragdakis, G. (2023). A tale of two markets: Investigating the ransomware payments economy. *Communications of the ACM, 66*(8), 74–83. https://doi.org/10.1145/3582489

Oz, H., Aris, A., Levi, A., & Uluagac, A. S. (2022). A survey on ransomware: Evolution, taxonomy, and defense solutions. *ACM Computing Surveys, 54*(11s), 1–37. https://doi.org/10.1145/3514229

Reshmi, T. R. (2021). Information security breaches due to ransomware attacks—A systematic literature review. *International Journal of Information Management Data Insights, 1*(2), 100013. https://doi.org/10.1016/j.jjimei.2021.100013

Robles-Carrillo, M., & García-Teodoro, P. (2022). Ransomware: An interdisciplinary technical and legal approach. *Security and Communication Networks, 2022*, 2806605. https://doi.org/10.1155/2022/2806605

Ruellan, E., Paquet-Clouston, M., & Garcia, S. (2024). Conti Inc.: Understanding the internal discussions of a large ransomware-as-a-service operator with machine learning. *Crime Science, 13*, 16. https://doi.org/10.1186/s40163-024-00212-y

Saccone, F., Melillo, P., Sgueglia, A., Di Sorbo, A., & Visaggio, C. A. (2025). The ransomware blueprint: Attack patterns and strategic variations across gangs. *Journal of Information Security and Applications, 95*, 104264. https://doi.org/10.1016/j.jisa.2025.104264

Taekema, S. (2021). Methodologies of rule of law research: Why legal philosophy needs empirical and doctrinal scholarship. *Law and Philosophy, 40*, 33–66. https://doi.org/10.1007/s10982-020-09388-1

Teichmann, F. (2026). International legal responses to ransomware: Toward a ban on payments? *International Cybersecurity Law Review, 7*, 41–68. https://doi.org/10.1365/s43439-025-00167-z

Teichmann, F. M. J., & Wittmann, C. (2023). When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. *Journal of Financial Crime, 30*(6), 1491–1498. https://doi.org/10.1108/JFC-04-2022-0093

Turner, A. B., McCombie, S., & Uhlmann, A. J. (2020). Discerning payment patterns in Bitcoin from ransomware attacks. *Journal of Money Laundering Control, 23*(3), 545–589. https://doi.org/10.1108/JMLC-02-2020-0012

U.S. Department of the Treasury, Office of Foreign Assets Control. (2021). Updated advisory on potential sanctions risks for facilitating ransomware payments. https://ofac.treasury.gov/recent-actions/20210921

Vakhitova, Z., & Mezzetti, C. (2026). Ransomware, emotions, and the decision to pay: Evidence from a factorial experiment. *Crime & Delinquency*. Advance online publication. https://doi.org/10.1177/00111287261440149

Vinogradskiy, Y., Schubert, L., Taylor, A., Rudoler, S., & Lamb, J. (2024). Radiation oncology ransomware attack response risk analysis using failure modes and effects analysis. *Practical Radiation Oncology, 14*(5), e407–e415. https://doi.org/10.1016/j.prro.2024.03.001

Welburn, J. W., & Strong, A. M. (2022). Systemic cyber risk and aggregate impacts. *Risk Analysis, 42*(8), 1606–1622. https://doi.org/10.1111/risa.13715

Whelan, C., Bright, D., & Martin, J. (2024). Reconceptualising organised (cyber)crime: The case of ransomware. *Journal of Criminology, 57*(1), 45–61. https://doi.org/10.1177/26338076231199793

Worsley, M. K., Kendall-Morwick, J., & Houston, K. A. (2025). Change waits for no one: An examination of the legal response to ransomware attacks. *Criminal Justice Policy Review, 36*(6), 259–280. https://doi.org/10.1177/08874034251363431

Yuryna Connolly, L., & Borrion, H. (2022). Reducing ransomware crime: Analysis of victims' payment decisions. *Computers & Security, 119*, 102760. https://doi.org/10.1016/j.cose.2022.102760