International Cybersecurity Law Review
https://doi.org/10.1365/s43439-025-00167-z

RESEARCH

International legal responses to ransomware: toward a ban on payments?

Fabian Teichmann

Received: 13 September 2025 / Accepted: 8 December 2025

Abstract Ransomware has matured into a transnational, profit-driven threat that exploits asymmetries in cyber resilience and legal frameworks. This article evaluates whether moving toward a legal prohibition on ransom payments is a viable and proportionate strategy. Using a comparative analysis of developments between 2023 and 2025 in the United States, United Kingdom, European Union and selected third countries (notably Australia), it maps emerging policy instruments—targeted payment bans, payment-preclearance/approval regimes, mandatory incident and payment reporting, and sanctions-based constraints—and assesses their interaction with existing international law, including the Budapest Convention and the draft UN Cybercrime Convention. The analysis highlights the deterrent rationale of "starving the business model" through reduced payment flows, while scrutinizing material risks: displacement effects across jurisdictions, potential under-reporting, operational harm to essential services, and disproportionate burdens on SMEs. It further addresses human-rights and due-process concerns (necessity, proportionality, narrowly tailored exemptions), conflicts of laws in multinational incidents, and the role of crypto-asset controls and coordinated law-enforcement disruption. The article proposes an incremental, internationally coordinated roadmap: (i) harmonized bans for governments and critical infrastructure; (ii) universal, time-bound reporting of incidents and payments; (iii) strengthened cross-border MLA/extradition and asset-freezing for ransomware proceeds; (iv) victim-support mechanisms (decryption sharing, recovery funding) to avoid perverse incentives; and (v) norms addressing safe havens. The central claim is that a payment ban can be effective only as part of a comprehensive framework that couples legal constraints with resilience, transparency, and multilateral enforcement; under those conditions, a converging

✉ Fabian Teichmann
London School of Economics, London, United Kingdom
E-Mail: F.M.Teichmann@lse.ac.uk

Published online: 19 January 2026

international norm of refusing to pay cyber ransoms is both legally tenable and strategically advantageous.

Keywords Cyber extortion · Incident reporting obligations · Sanctions-based enforcement · Critical infrastructure protection · International cybercrime law

1 Introduction

Ransomware has evolved into a global cybersecurity epidemic over the past decade, causing billions in economic damage and disrupting critical services worldwide. This form of cyber extortion—where malware is used to encrypt or steal data until a ransom is paid—is "the fastest growing type of cybercrime", projected to cost victims an estimated $265 billion annually by 2031[15]. High-profile attacks on hospitals, pipelines, and government agencies across multiple countries have underscored the urgent threat. A core reason ransomware persists is simple: it is lucrative. As one cybersecurity official bluntly stated, *"money drives ransomware"*—criminals are financially motivated, and as long as victims continue to pay ransoms, attackers will have incentive to keep launching these attacks [10]. This dynamic has prompted intense debate over how criminals launder the proceeds of their crimes and how law and policy should respond [20, 20–37, 40, 43].

One increasingly discussed idea is to "break the hacker profit model" by cutting off ransom payments entirely. If victims were legally barred or strongly dissuaded from paying, ransomware might become a far less attractive crime. Indeed, governments and experts worldwide have begun considering measures such as banning ransom payments or mandating that incidents and payments be reported to authorities. In the United States, for example, the White House in 2023 openly considered an outright ban on ransomware payments, reflecting a reversal from its earlier stance [10, 15]. The United Kingdom launched a 2025 policy consultation on prohibiting certain organizations from paying and on requiring transparency around ransomware attacks [3]. Australia went a step further by enacting a first-of-its-kind law in 2024 that requires organizations to report any ransomware payment within 72 h, aiming to shine light on the problem [6]. Yet, these efforts raise complex questions: Would banning payments actually reduce ransomware, or would it create new problems? How can any one country's law be effective against a transnational threat? And are such measures consistent with international law, including cybercrime conventions and human rights norms?

This article examines the emerging international legal and policy responses to the ransomware epidemic, focusing on proposals to ban ransom payments or mandate incident disclosures. It takes a comparative lens across key jurisdictions—including the US, UK, EU, and others—to analyze recent developments from 2023–2025. It also evaluates the implications under existing international law (such as cybercrime treaties) and the challenges of coordinating a global response. In doing so, we consider both the potential benefits of prohibiting ransom payments (notably, undermining the criminals' business model) and the potential drawbacks or unintended consequences (such as increased harm to victims or difficulties in enforcement).

Finally, the discussion explores how an international treaty or coordinated framework might address ransomware, and whether a global consensus is forming toward a norm of refusing to pay cyber ransoms. The goal is to assess, from a legal perspective, whether moving "toward a ban on payments" is a viable and effective strategy in combating the ransomware epidemic.

2 The ransomware epidemic and the role of payments

Ransomware is a form of cybercrime where attackers infiltrate an IT system, encrypt data or threaten to leak sensitive information, and demand a ransom (typically in cryptocurrency) for decryption keys or a promise not to publish the data [35, 38, 39, 41, 42, 45]. This criminal business model has proven devastatingly effective. By denying organizations access to their own data—or by threatening costly data breaches—ransomware attackers place victims in an agonizing position where paying the extortion may seem like the quickest way to mitigate damage. Globally, hundreds of millions of dollars are paid to ransomware gangs each year. In fact, 2023 saw a record $1.25 billion in known ransomware payments, though that figure dropped to about $814 million in 2024 (a 35% decline) as more victims refused to pay and law enforcement disrupted major gangs. Despite the slight downturn in revenue, the overall frequency of ransomware attacks has not abated—if anything, incidents spiked in late 2024 even as fewer victims paid up [47]. These trends highlight that ransomware remains highly profitable, but also that determined efforts (both by authorities and victims) can influence attackers' success.

The decision to pay or not pay ransom is at the heart of ransomware's legal and ethical dilemma. On one hand, paying a ransom can sometimes restore systems quickly, potentially sparing a company's operations or a public agency's services (e.g. getting a hospital back online to treat patients). On the other hand, each payment furthers a cycle that funds and encourages more crime. As an Australian cybersecurity official observed, ransomware is *"a financially motivated crime, and the more you pay the more you generate the interest in further criminal activity of that kind"* [10]. In other words, ransom payments fuel the ransomware epidemic—they act as a "key financial pipeline" for cybercriminal networks [3]. Law enforcement worldwide, including the FBI and Europol, have long discouraged victims from paying ransoms, noting there is never a guarantee that criminals will honor their promises (decrypting data or refraining from leaks) and that payment may even mark an organization as a repeat target. Indeed, repeat victimization and "double extortion" (where attackers both encrypt data and steal it for leverage) have become common.

Crucially, paying a ransom is generally not illegal for private parties under most national laws. Unlike the clear illegality of the hackers' actions, a victim's act of paying the extortion demand occupies a gray area. In the United States, for example, "no federal statutes expressly criminalize making ransomware payments" [18]. Victims are free (from a criminal law standpoint) to pay an unsanctioned cybercriminal to restore their data. Similarly, most countries—including EU member states and Commonwealth countries—have no law forbidding private ransom payments, apart

from general prohibitions on financing terrorism or sanctions violations. *However, this permissive legal stance is changing.* Governments are grappling with whether allowing payments is tenable in the face of a global ransomware wave. The logic is analogous to longstanding counter-terrorism policies: just as many states (and UN Security Council resolutions) urge not paying ransoms to terrorists in kidnapping cases [46],so too might paying cyber-ransoms be outlawed to choke off criminals' funding. The following sections survey how different jurisdictions have begun to respond—through bans, reporting mandates, and other measures—and set the stage for a discussion on international coordination.

3 National policy responses: bans and reporting mandates

3.1 United states: debating a prohibition and enhancing reporting

In the United States, ransomware policy has been in flux in recent years. There is currently no federal law outright banning ransom payments by victims, but the idea has gained traction in policy circles. In May 2023, the Biden Administration signaled it was considering an unprecedented federal ban on ransomware payments. Anne Neuberger, Deputy National Security Advisor for Cyber, revealed that the White House—in concert with international partners in the International Counter Ransomware Initiative (CRI)—was examining whether prohibiting payments (with certain waivers) could help counter financially motivated threat actors. This marked a notable shift, as the Administration had previously stopped short of supporting a ban. In fact, as recently as late 2022, U.S. officials decided *against* an outright ban, reasoning that a premature prohibition might backfire: *"We'd essentially be pressing victims to make their payments go underground",* Neuberger warned at the time. The concern was that if paying a ransom were illegal, companies might still pay but attempt to hide the transaction, resulting in even less transparency and reporting of attacks. Such unintended consequences temper the U.S. debate—even proponents acknowledge a ban, if implemented too hastily, could cause "victims to cover up every ransomware attack", creating a false impression of progress while the crime continues unabated underground [10].

Despite these hesitations at the federal level, the U.S. has taken steps to strongly discourage ransom payments through other means. One significant factor is sanctions law: Federal regulations *prohibit* any transactions with individuals or groups on the U.S. Treasury's sanctions list. This means if a ransomware gang is linked to a sanctioned entity (for example, a group tied to a country under sanctions or designated terrorists), paying them could "implicitly make [the] ransomware payment a crime" under existing laws. The U.S. Treasury's Office of Foreign Assets Control (OFAC) issued advisories in 2020 and 2021 emphasizing that companies paying ransoms to certain threat actors risk violating sanctions, and that the government "strongly discourages" any ransom payments [18]. Additionally, the U.S. Financial Crimes Enforcement Network (FinCEN) has guided financial institutions to treat ransomware payments as suspicious and reportable. In effect, while paying

cyber ransoms is not outright banned for victims, it is highly discouraged and can be legally perilous if the attacker is on a sanctions list or has terror connections.

At the same time, the U.S. is moving toward mandatory reporting of ransomware incidents and payments, especially for critical sectors. In March 2022, Congress passed the Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA), which (once regulations are finalized) will require companies in designated critical infrastructure sectors to report substantial cyber incidents within 72 h and to report any ransomware payment within 24 h to the Cybersecurity and Infrastructure Security Agency (CISA). This law, when fully implemented (expected by 2024–2025), will create a federal reporting regime somewhat analogous to Australia's (discussed below), though focused on critical industries. Even ahead of CIRCIA's implementation, sectors like pipelines have had ad-hoc mandates (after the 2021 Colonial Pipeline ransomware incident, the Transportation Security Administration ordered pipeline operators to promptly report incidents). The broader goal is to ensure the government gets rapid notification of ransomware attacks and payments, enabling law enforcement to respond, warn others, and gather intelligence on the actors. U.S. policymakers believe better data on ransomware incidents will improve coordination and shine a light on the scope of the problem, countering the underreporting that has plagued cybercrime statistics [18].

It is also worth noting that some U.S. state governments have already imposed targeted bans on ransom payments within their jurisdictions. North Carolina broke ground in 2022 by banning all state and local government agencies from paying ransoms or even negotiating with ransomware actors [10]. Shortly thereafter, Florida enacted a similar law prohibiting state agencies and municipalities from paying cyber ransoms, making it the second state to do so [17]. (Tennessee and others have likewise explored or enacted restrictions for the public sector) [12, 13]. These state-level laws aim to protect taxpayer funds and disincentivize attacks on public infrastructure. However, early evidence from North Carolina suggests the deterrent effect may be limited—the number of reported attacks on NC public entities did not notably decrease after the ban [10]. Ransomware gangs may still target government units, either hoping the victim will find a workaround or simply to cause disruption. The mixed results underscore that an isolated ban in one state or sector can be circumvented or may shift attackers' focus rather than stop them outright.

U.S. officials continue to debate the merits of a broader payment ban. In April 2024, a Congressional hearing underscored both the appeal and the risks of such a policy. Kemba Walden, former Acting National Cyber Director, testified that while a ransomware payment ban remains the "ultimate goal" or "North Star" for curbing criminals' leverage, the country is not yet prepared to implement it. Walden explained that the U.S. economy—particularly small businesses and critical service providers like rural hospitals—lacks the resilience to withstand a ban at present. If companies had no legal option to pay, many might face catastrophic losses or even bankruptcy following a major ransomware attack. *"If we banned ransomware payments today, we could bankrupt the very small- and medium-sized businesses that the American economy relies upon",* Walden cautioned, giving the example of small rural hospitals that might be forced to shut down after an incident if unable to pay for quick restoration. She and other experts argued that prohibiting payments now

won't stop attacks from happening; it would chiefly "starve" the victimized businesses rather than the criminals if those businesses are not cyber-resilient. The panel instead advocated a phased approach: improve baseline cybersecurity and incident response across the economy, provide support (grants, insurance reforms, technical aid) to "cyber-poor" organizations, and intensify disruption of ransomware gangs. Only after "shifting the balance"—making attacks less profitable and companies better prepared—would a payment ban become a viable tool [4]. In essence, the U.S. is hedging: keeping the option of a future ban open, but focusing current efforts on mandatory reporting, bolstering defenses, and international law enforcement collaboration, as discussed later.

3.2 United kingdom: toward a targeted ban and new reporting regimes

The United Kingdom has been grappling with a surge of ransomware attacks and is now moving decisively toward stricter legal curbs on ransom payments. In early 2023, the UK government launched a public consultation on proposals to reduce ransom payments and increase incident reporting [3]. By January 2025, the Home Office set out an ambitious plan described as an "entirely new approach" to ransomware, aimed at *"disrupting the business model"* of cyber-extortionists [1, 14]. The UK's proposals, which align with its global leadership in the Counter Ransomware Initiative, consist of three main pillars [6]:

1. Ban on Ransom Payments by Critical Sectors: A targeted ban would extend the existing prohibition on central government agencies (which already cannot pay ransoms) to all public sector bodies and owners/operators of Critical National Infrastructure (CNI). In practice, this means government departments, local authorities, the National Health Service, schools, and essential utilities like energy, water, finance, telecoms, transportation and others would be barred from paying if hit by ransomware. The rationale is to protect services vital to the public and to remove the incentive for attackers to single them out. If criminals know that UK hospitals or infrastructure operators *"will make no money"* from attacks, those targets should become less attractive. Notably, the government has even asked whether key suppliers to those critical sectors (e.g. IT providers or data center vendors serving CNI organizations) should also be included under the payment ban, given how interwoven supply chains are. This broad approach aims to close loopholes (attackers might otherwise target a critical sector via a contractor) and follows precedents set by other countries. In fact, in the 2023 joint statement of the international Counter Ransomware Initiative, dozens of countries—led by the UK and U.S.—agreed that no central government funds should be used to pay ransoms. The UK's ban would implement that principle domestically and arguably take it further by covering local government and critical industry operators.
2. Ransomware Payment "Approval" Regime for Others: For organizations *not* covered by the above ban (i.e. private companies outside critical infrastructure), the UK proposes a new "ransomware payment prevention" regime. This would require any victim considering paying a ransom to first report their intention to a government authority, who would then assess the situation and potentially block the

payment in certain cases. In essence, it's a mandatory notification and oversight system before a ransom transaction occurs. Under the proposal, once a company notifies the authorities that it intends to pay a ransom, it would receive support and advice on alternatives (for example, help with recovery, using backups, engaging cybersecurity experts). The authorities would also review whether the proposed payment should be prohibited—for instance, if the payment would violate sanctions or anti-terrorism financing laws (e.g. the ransom demand is linked to a sanctioned hacker group). If no clear legal reason to block exists, the ultimate decision to pay or not would still rest with the victim organization, but at least the incident would be on record and law enforcement could potentially monitor the outcome. This novel approach tries to strike a balance: it doesn't ban all private-sector payments (recognizing that an absolute ban could be too blunt), but it inserts government oversight into the process. Over time, this could discourage payments by adding friction and scrutiny. It also ensures that even when payments occur, they are not kept secret—addressing the underreporting issue. However, such a regime would be complex to implement; it essentially creates a licensing system for paying ransoms, which is unprecedented in cyber contexts. The government has sought feedback on how to make this workable and what sanctions for non-compliance would be appropriate (ranging from criminal penalties for paying without reporting, to fines or even director disqualifications for flouting the rules) [3].

3. Mandatory Ransomware Incident Reporting: Complementing the above, the UK intends to mandate reporting of ransomware incidents across the board. This means any organization hit by a ransomware attack (regardless of whether they pay or not) would be required by law to report the incident to the relevant authorities (likely the National Cyber Security Centre (NCSC) or law enforcement) within a specified time frame. The goal is to ensure *"full transparency of the ransomware threat landscape"*, enabling the UK's National Crime Agency and NCSC to gather intelligence, support victims, and coordinate responses [6]. Greater reporting can help authorities track ransomware trends, link campaigns, and possibly warn other potential targets (for example, if a widespread exploit is being used). It also dovetails with the payment oversight regime—since even if a victim decides not to pay, the fact that an incident occurred should still be known to regulators. The UK already has some reporting requirements for data breaches (under GDPR, organizations must report personal data breaches within 72 h to the Information Commissioner's Office) and certain sectors like finance have cyber incident reporting rules. But this proposal would create a more comprehensive ransomware-specific obligation. It mirrors approaches like the EU's NIS2 Directive (discussed below) and Australia's new law. By institutionalizing incident reporting, the UK aims to remove the stigma or reluctance companies have about coming forward and make ransomware a more manageable, measurable menace.

By July 2025, these proposals enjoyed broad government support. The Home Office indicated it would move forward to implement a "targeted ban on ransomware payments" for public sector and critical infrastructure, along with the complementary prevention and reporting measures [7, 11]. A UK Government response in mid-

2025 confirmed plans to draft legislation effecting these changes. It's notable that there is cross-party consensus in the UK on taking stronger action—a May 2024 proposal under the previous Conservative government similarly sought to require all ransomware incidents to be reported and even to force victims to obtain a government license before paying. That specific licensing idea evolved into the current "report-before-paying" regime under the Labour government in 2025, but the continuity shows a sustained political will to tackle ransomware. UK officials argue these steps will *"strike at the heart of the cybercriminal business model"* by cutting off funds [6]. As Home Office Minister Dan Jarvis put it, the aim is to "hit these criminal networks in their wallets and cut off the key financial pipeline they rely upon" [3].

From a legal perspective, the UK's approach raises important considerations. The narrowed scope of the outright ban (limiting it to public sector and CNI) is designed to protect the most vital services and taxpayer money, while avoiding the potentially harsh impact of a blanket ban on all businesses. Private companies would still have a (heavily discouraged) option to pay, but under oversight. The introduction of prior notification and potential blocking of payments is a distinctive regulatory innovation—effectively treating a ransom payment somewhat like a suspicious financial transaction that can be interdicted. Compliance and enforcement will be challenging: companies may fear reputational damage or regulatory consequences and thus might be tempted not to report either an incident or an intent to pay. The UK proposals consider penalties for non-compliance to address this, such as fines or even making it a criminal offense for executives to secretly pay ransoms when prohibited [3]. If legislation passes, the UK will join the forefront of countries using law not just to punish cybercriminals (which has always been the case) but to actively shape the behavior of victims in responding to cybercrime. This represents a significant evolution in cyber law strategy.

3.3 European union and member states: emphasis on reporting and resilience

At the level of the European Union, there is currently no union-wide ban on ransom payments, and most EU member states do not criminalize paying ransoms to cybercriminals (absent links to terrorism or sanctions). Instead, Europe's approach has emphasized improving cybersecurity resilience and transparency. The marquee development is the EU's Network and Information Security Directive 2 (NIS2), adopted in 2022 and taking effect from late 2024 [44]. NIS2 is a comprehensive cybersecurity law that applies to a broad range of "essential" and "important" entities across EU member states (including sectors like energy, transport, health, banking, infrastructure, digital providers, and more). Among its many requirements, NIS2 mandates that covered organizations report significant cyber incidents—including ransomware attacks—to authorities within a very short timeframe (often 24 h for initial notice) [6]. By requiring immediate notification of incidents, the EU aims to speed up incident response and facilitate cross-border coordination (via a network of national CSIRTs and a central EU cyber unit). In practice, if a hospital in Germany or a bank in France suffers a ransomware breach, they must alert regulators almost right away, who can then alert Europol or other member states if needed. While NIS2 does not force disclosure of ransom *payments* specifically, any ransomware incident

significant enough to impact services or data likely triggers the reporting duty, meaning authorities will become aware and can inquire if a ransom demand was made or paid. This indirectly increases government visibility into ransom payments without explicitly banning them. EU officials have noted that faster reporting will help build a fuller picture of the ransomware threat and possibly deter companies from quietly paying criminals without informing law enforcement.

Individual EU countries largely echo the stance of discouraging payments but stopping short of outlawing them. Law enforcement agencies (like France's ANSSI or Germany's BSI) regularly advise against payment on principle. In France, a law was debated in 2021 to ban ransom payments and prohibit insurers from reimbursing them (amid concern that cyber insurance was enabling criminals), but the adopted measure was softer—requiring companies to report the attack to law enforcement if they want to deduct the payment as an expense or claim insurance reimbursement. Thus, transparency was again the focus: France basically said you can't quietly pay and get insurance coverage unless you involve the police. Other nations like Germany and Netherlands have robust incident reporting cultures and often public-private information-sharing of ransomware cases (through sectoral ISACs, etc.), but no explicit payment bans. An interesting data point in Europe is that many victims are refusing to pay lately—for instance, a prominent 2022 attack on Ireland's national health service (HSE) saw the government refuse the ransom and work with international experts to recover, albeit at high cost. Similarly, several large European companies hit in 2023 opted not to pay and instead endured data leaks, citing policies of non-payment. This suggests that a norm against paying is taking hold in practice, even if not codified in law.

At the European Union level, there is also increasing diplomatic coordination on ransomware. The EU has attributed major ransomware attacks to state-tolerated criminal groups and even imposed sanctions on certain cyber actors. In 2022 the EU sanctioned individuals linked to the WannaCry, NotPetya, and other attacks (some of whom were involved in ransomware campaigns), thereby legally barring any EU person or company from transacting with them (which includes paying ransom). Furthermore, Europol's European Cybercrime Centre (EC3) has been actively coordinating multinational operations against ransomware gangs. One notable success was "Operation Cyclone" against the DoppelPaymer group in early 2023, involving law enforcement from Germany, Ukraine, and others to arrest suspects and seize infrastructure. In 2023–2024, Europol also supported a joint operation that disrupted the prolific LockBit ransomware gang, in coordination with the FBI and UK's NCA, leading to seizures of servers and even some arrests. These enforcement actions, coupled with anti-money-laundering regulations for cryptocurrencies, have contributed to the decline in ransomware payments observed in 2024 [47]. EU officials have thus tended to frame the solution to ransomware in terms of "enhancing resilience, improving reporting, and bolstering law enforcement cooperation", rather than banning payments outright. However, as the ransomware threat remains acute, it is possible the EU could consider stronger measures in the future, especially if spurred by key member states or if a unified international stance emerges.

It should be noted that EU policy discussions in 2023–2025 did touch on ransomware payment bans in some forums. For example, the idea of prohibiting pay-

ments was raised in the context of EU-UK cybersecurity cooperation. In a December 2024 EU-UK joint cyber dialogue, officials discussed deterrence strategies against ransomware and mentioned the UK's legislative proposals as a potential model [6]. The European Council has also included ransomware in its declarations, emphasizing that no effort should be spared to stop ransomware actors—though without explicitly endorsing or rejecting payment bans. Private sector voices in Europe are increasingly supportive of stricter measures; a 2023 survey by the Canadian Internet Registration Authority (CIRA) found almost two-thirds of cybersecurity professionals (many in North America and Europe) favor legislation prohibiting ransom payments [8]. Companies are frustrated by the incessant attacks and some believe only government intervention can resolve the "prisoner's dilemma" of individual firms choosing to pay. Still, until there is an EU consensus, member states are likely to continue with the current mix of mandatory reporting (NIS2), sanctions enforcement, and strong discouragement of payments as the de facto policy.

3.4 Australia: mandatory ransom payment reporting—A pioneering law

Australia emerged by 2024 as a trailblazer in ransomware policy by introducing one of the world's first legal requirements targeting ransom payments. After a series of high-profile cyberattacks on Australian companies (including a major telecom and a health insurer in 2022) that exposed millions of citizens' data, the Australian government vowed to get tougher on ransomware. This led to the passage of the Cyber Security Act 2024 (Cth), which took effect on 30 May 2025 and mandates that all organizations report any ransomware or cyber extortion payment within 72 h [6]. The law covers businesses operating in Australia above a modest size threshold (annual turnover of AUD $ 3 million or more) as well as entities responsible for critical infrastructure assets. In essence, if a covered business makes a payment in response to a cyber incident—or even if a third party (like their insurer or a negotiator) pays on their behalf—that payment must be reported to the government (specifically, to the Australian Signals Directorate's cyber reporting portal) within three days. The required report includes detailed information: the amount paid (or benefit given), the timing and method, the attacker's demands and any communications, and a description of the incident itself [2].

Importantly, Australia's law does not prohibit the act of paying a ransom; it stops short of criminalizing payments. Instead, it aims for transparency and data-gathering. The premise is that by compelling disclosure of ransom payments, authorities can better understand the scale of the ransomware problem, assist victims, and potentially track the flow of funds (especially since payments are often in cryptocurrency). The Australian government felt that many ransom incidents were being hidden from regulators and the public, undermining efforts to combat the crime. The new reporting mandate seeks to end that secrecy. Companies that fail to report a ransomware payment face penalties—specifically, a civil fine of up to 60 penalty units (currently AUD $ 19,800) per violation. While not enormous, this fine and the prospect of regulatory enforcement provide incentive to comply. The law includes a six-month grace period (until the end of 2025) where regulators will emphasize education over punishment, and after that, a more aggressive enforcement stance will kick in [2].

To address industry concerns, Australia's legislation built in "limited use" protections for the reported information. This means data submitted in a ransomware payment report can generally only be used by the government for certain purposes: responding to or investigating the incident, mitigating cybersecurity threats, national security or intelligence activities, or related enforcement actions. Crucially, the law tries to reassure companies that if they self-report a payment, the details won't be used to automatically prosecute or penalize them for having been attacked or for the fact of paying. (Since paying is not outlawed, the main legal risk would be if the payment violated sanctions or other laws, and the government has indicated good-faith reporting will not be used as a "gotcha" for unrelated infractions.) This approach seeks to strike a balance: encouraging openness without overly frightening victim organizations that disclosure will lead to lawsuits or reputational damage. In addition, Australia established a new Cyber Incident Review Board—akin to the U.S. Cyber Safety Review Board—to analyze major incidents in a "no fault" manner and make public recommendations for resilience [6]. The hope is that lessons learned from ransomware cases (especially patterns gleaned from the influx of payment reports) will inform better defensive measures nationwide.

Australia's mandatory reporting law has significant implications. It effectively makes Australia a test case for whether transparency alone (without a payment ban) can reduce ransomware. By knowing who paid and how much, Australian authorities can identify if particular gangs are heavily targeting their companies and possibly coordinate law enforcement action. It also creates an official record that could feed into international efforts (e.g. sharing anonymized data with partners to track cryptocurrency wallets used by ransomware groups). Early commentary suggests other jurisdictions are watching closely; the law firm Hogan Lovells noted that Australia's move *"leads a new era"* and other countries might follow its lead in introducing similar requirements. Indeed, the UK consultation in 2025 explicitly referenced Australia's approach as a model for improving incident reporting. The Australian government frames the law as pro-business in the long run, reasoning that a company which aligns with this reporting regime will be better prepared if (or when) other jurisdictions adopt comparable rules [2].

From an international legal standpoint, Australia's law does not conflict with any treaty obligations since it doesn't prohibit anything already allowed; it simply imposes a domestic reporting duty. Businesses operating in Australia (even if foreign-owned) now have to consider this in their incident response plans—for example, a U.S. company with an Australia branch that pays a ransom affecting that branch would need to report to ASD within 72 h, potentially raising cross-border complexities (especially if U.S. authorities also require notification under forthcoming CIRCIA rules). It exemplifies the trend of domestic legislation addressing ransomware in innovative ways, contributing to a patchwork of laws that multinational companies must navigate.

3.5 Other jurisdictions and global initiatives

Beyond the above examples, numerous other jurisdictions have been reexamining their laws and policies in light of the ransomware epidemic:

- Canada: As of 2025, Canada has not banned ransomware payments, but the federal government explicitly *"does not recommend paying ransom"*, as any payment "fuels the ransomware model" [16]. Canadian law enforcement (the RCMP and Canadian Centre for Cyber Security) urge victims to report incidents and avoid paying. Canada has debated mandatory reporting of ransom payments; a 2023 bill was floated to require companies over a certain size to report payments (similar in spirit to Australia's law) [19]. There is also discussion of updating anti-money laundering laws to penalize paying ransoms if the funds flow to criminal organizations. As of this writing, however, no specific federal law compels disclosure or bans payment, so the approach remains advisory. Interestingly, a survey in Canada found a strong majority of cybersecurity professionals would support making ransom payments illegal [8], indicating a potential shift in public opinion that legislators could eventually heed.
- Israel, Singapore, and Others: Israel faced an onslaught of ransomware in 2021–2022 and considered requiring companies to report attacks to a government authority, but enforcement mechanisms remain voluntary for most sectors. Singapore co-leads the CRI's effort on ransomware policy (with the UK), and while it has not banned payments, it has tightened regulations on cryptocurrency exchanges to enforce stricter KYC (know-your-customer) rules, aiming to make it harder for ransomware actors to cash out illicit gains. Some countries like United Arab Emirates have cybersecurity regulations requiring breaches (including ransomware incidents) to be reported to regulators in certain sectors (finance, critical infrastructure), but no explicit ransom payment laws. Japan and South Korea have seen major ransomware incidents but have focused on strengthening cyber defenses and information-sharing rather than payment bans.
- International Counter Ransomware Initiative (CRI): This U.S.-led multilateral coalition, launched in 2021, has grown to 68 member countries plus the EU. It serves as a forum for coordinating ransomware response strategies. In 2023–2024 the CRI developed a "Resilience and Counter Illicit Finance" working group that specifically looks at policies to reduce ransom payments globally. Notably, in January 2024, all CRI member nations jointly declared that government institutions under their authority should not pay ransomware extortion demands [6]. This public commitment essentially sets an international norm (at least among allies) that taxpayer funds will not be used to reward cybercriminals. The CRI also endorsed best practices in October 2024, in collaboration with the insurance industry, to encourage alternatives to paying ransoms, emphasizing backup restoration and expert incident response instead [3]. While the CRI statements are non-binding, they represent a coordinated political stance and have likely influenced national policies (as seen with the UK and others referencing the CRI in their plans). The CRI is moving toward further initiatives in 2025, such as sharing information on cryptocurrency wallets used by ransomware gangs and promoting *"secure by design"* software to reduce vulnerabilities. This initiative underscores that ransomware is being treated not just as a domestic criminal issue but as a shared international security challenge requiring collective action.

- Sanctions and Law Enforcement: On the global stage, coordinated law enforcement has begun to make a dent in ransomware operations. Multi-country efforts through Interpol, the Budapest Convention network, and intelligence sharing have led to arrests of ransomware actors in Eastern Europe and elsewhere. The U.S., EU, and UK have each imposed sanctions on ransomware actors and the cryptocurrency exchanges or "mixers" that launder their proceeds. For instance, the U.S. sanctioned the crypto mixer Tornado Cash in 2022, and in 2023 Chainalysis reported a "substantial decline" in the use of mixers by ransomware gangs as a result [47]. This shows that economic levers can influence criminal behavior—relevant to the debate on banning payments. If criminals find it harder to move or spend their ransom profits due to sanctions and surveillance, the incentive to launch attacks diminishes. That said, the biggest challenge remains ransomware safe havens: countries like Russia (home to many ransomware gangs) and North Korea (whose state-backed hackers engage in ransomware to fund the regime) have not participated in global efforts. The proposed UN Cybercrime Convention (discussed next) and ongoing diplomatic pressure seek to bring these holdouts into the fold, or at least make it harder for them to harbor cybercriminals with impunity [9].

In summary, while approaches vary, the clear trend from 2023 onward is toward more assertive measures to curb ransomware payments and increase transparency. Only a few jurisdictions have moved to outright bans (largely for government entities), but many are considering it, and reporting mandates are becoming more common. The stage is set for a larger international conversation on harmonizing these strategies, which we turn to now.

4 International law implications and cross-Border challenges

4.1 Consistency with cybercrime treaties and norms

Any national law or policy addressing ransomware operates against the backdrop of existing international legal instruments on cybercrime. The primary treaty in this domain is the Council of Europe Convention on Cybercrime (Budapest Convention) of 2001, which over 85 countries (including the US, EU states, and others) have joined. The Budapest Convention and its recent Second Protocol do not explicitly address ransom payments by victims—rather, they require criminalization of offences like computer intrusion, data interference, and cyber extortion (which covers the acts ransomware criminals commit) and facilitate cross-border cooperation in investigation and prosecution. For example, a ransomware attack entails multiple Budapest offenses (illegal access, system interference, data interference, and often computer-related fraud/extortion); under the treaty, each party must have laws to prosecute these acts and must assist other countries' investigations (through extradition, mutual legal assistance, etc.). The Convention's Guidance Note on Ransomware (2022) reaffirmed that its provisions are flexible enough to tackle ransomware cases—and

that tools like the new protocol (which streamlines obtaining electronic evidence across borders) will improve enforcement [5].

Measures like banning ransom payments or mandating reports are not mandated (or prohibited) by the Budapest Convention, since those measures concern victim behavior and incident response rather than criminalizing the perpetrators. However, such measures complement the Convention's objectives by potentially reducing the incidence of cybercrime and encouraging cooperation with law enforcement. One could say they further the "spirit" of international cybercrime norms, which is to diminish cybercriminals' rewards and enhance collective security. There is no conflict between a country banning payments and its Budapest obligations, as paying ransom is not a protected right or requirement in any treaty. Likewise, mandatory reporting of incidents aligns with Budapest Convention Article 35, which encourages prompt sharing of information with other jurisdictions about cyber threats.

A newer player on the scene is the proposed United Nations Convention on Countering the Use of ICTs for Criminal Purposes, often shortened to the UN Cybercrime Convention. This treaty was originally tabled by Russia but has since seen wide negotiation through a UN Ad Hoc Committee, with a draft adopted by the UN General Assembly in late 2024. The convention aims to create a global framework for cooperation on cybercrime, including ransomware, that would include countries like Russia and China (which are outside the Budapest Convention). The United States and EU decided to support the treaty despite initial misgivings, hoping it can be leveraged to fight ransomware globally. The draft text (as known in 2024) obliges states to criminalize core cyber offenses and improve cooperation, much like Budapest, though there are concerns it could be misused by authoritarian regimes to justify crackdowns. From the perspective of ransomware policy, the UN convention could be a vehicle to propagate norms about not paying ransoms. Even if the treaty itself won't ban payments (that would be outside its scope, which focuses on criminalizing offenders), it fosters *international collaboration that can indirectly support payment bans*. For instance, if all countries cooperate to investigate ransomware networks and trace ransom flows, the likelihood of catching perpetrators increases, which in turn strengthens the credibility of a no-payment stance (victims might refrain from paying if they trust that law enforcement can help recover systems or that attackers might be caught). U.S. officials indicated they see the UN treaty as having *"the potential to make improvements in international law enforcement cooperation to fight cybercrime",* including ransomware. They also hope to use it to address the issue of safe havens—pressing countries that "have allowed criminal ransomware groups to operate" to either cooperate or face censure [9]. In effect, the treaty could enshrine an expectation that states should not knowingly harbor ransomware operations, which dovetails with efforts to cut off ransom payments (because as long as certain states shelter the culprits, merely banning payments elsewhere may not suffice).

Beyond treaties, there are emerging international norms and non-binding agreements relevant to ransomware. For example, the G7 and G20 have issued communiqués condemning ransomware and calling for improved information sharing. The G7 in 2021 endorsed the view that ransom payments fuel further attacks and encouraged companies to harden defenses instead. The Paris Call for Trust and Security in

Cyberspace (2018), a multi-stakeholder declaration, includes combating cybercriminal activities like ransomware as a priority for international cooperation (though it doesn't mention payments specifically). Meanwhile, the UN Open-Ended Working Group (OEWG) on ICT security has discussed ransomware as a threat to critical infrastructure, indirectly supporting norms such as not targeting hospitals (a norm for state actors that one could argue cybercriminals should also abide by). While these broader initiatives do not directly impose rules about paying ransoms, they contribute to a climate where refusing to pay and refusing to tolerate cyber extortion is seen as the ethically right and secure course of action.

Interestingly, we might be witnessing the early formation of a global norm against ransom payments by governments at least. The Counter Ransomware Initiative's joint commitment that national governments won't pay is akin to the consensus against paying terrorist ransoms (as per UNSC Resolution 2133) [46]. If that norm holds and more countries adopt it, ransomware gangs will know that attacking government agencies will likely not yield profit—possibly deterring such attacks. The next step could be extending the norm to critical infrastructure and private sector best practices, though doing so formally would likely require either a broad international agreement or simultaneous national legislations. Some experts have even suggested a future protocol or annex to an existing treaty (like Budapest) focusing on ransomware, where signatories might pledge to outlaw payments above a certain amount or to certain types of attackers, but such an idea is still speculative.

In summary, current international law (Budapest Convention, etc.) is fully compatible with—and indeed supportive of—efforts to curb ransomware payments, even if it doesn't mandate those efforts. The main focus of treaties is to go after the criminals, not the victims, but the evolving practice of states shows a willingness to also regulate victim responses for the greater good. Ensuring consistency with human rights and other legal norms will be important (discussed below), but from a pure cybercrime law standpoint, countries have leeway to prohibit ransom payments under their domestic law without breaching any international obligations. They simply need to do so in a way that still encourages reporting and cooperation rather than driving the issue into the shadows. This interplay between national initiatives and international frameworks sets the stage for whether a more formal global consensus can emerge.

4.2 Cross-Border enforcement and coordination challenges

Ransomware is quintessentially a transnational threat. The attackers and their infrastructure are often in a different country (or multiple countries) from the victim, and the ransom payment typically moves across borders through global cryptocurrency networks. This poses huge challenges for enforcement and for any legal measures that stop at a nation's borders. If one country bans payments, determined victims or intermediaries might route payments through other jurisdictions. Likewise, if one country aggressively pursues a ransomware gang, the gang may simply shift operations to a more permissive jurisdiction. Effective response, therefore, demands international coordination at multiple levels.

One major challenge is the existence of "safe havens" for ransomware groups. As noted, many top-tier ransomware gangs operate from Russia or other states with tense relations with the West, where they face little risk of arrest so long as they do not target domestic entities or certain allies. This geopolitical wrinkle means that even if most of the world unites in not paying ransoms, a regime like Russia might quietly encourage these attacks as a form of pressure or simply turn a blind eye because it brings illicit revenue into their economy. The U.S. National Security Council and allies have repeatedly called out countries that *"allow criminal ransomware groups to operate"* within their borders [9]. However, without cooperation from those governments, legal measures like payment bans may have limited impact on the criminals themselves—they will continue launching attacks, possibly focusing on victims outside the no-pay club. In the worst case, if, say, NATO/EU countries all banned payments, ransomware actors might concentrate on targets in Asia or Latin America that still pay, or double down on exfiltrating sensitive data to extort victims via public leaks rather than encryption. Cross-border enforcement is thus critical: the more that all nations can cooperate to investigate, extradite, or otherwise disrupt ransomware actors, the fewer havens will remain. This is why the global reach of the budding UN Cybercrime Convention could be significant if it brings countries like Russia into a cooperative framework—although skeptics worry those states might still not earnestly help against groups they tacitly protect.

Another coordination challenge relates to jurisdiction and conflicts of law. Consider an example: a multinational company is hit by ransomware in Country A (which bans payments), but its IT department in Country B (which has no ban) wants to pay the ransom to restore global systems. Or a scenario where the decryption service is only accessible via infrastructure in Country C. Such multi-country incidents raise questions: whose law applies? If the company's headquarters are in a country that forbids payment, can it legally instruct a subsidiary abroad to pay? Could that be viewed as evasion? These complex situations will arise more as disparate laws proliferate. International law doesn't yet offer clear answers; it falls to conflict-of-law principles and perhaps future agreements to harmonize approaches. An international treaty specifically on ransomware could, for example, include an article that states agree not to view facilitating a ransom payment as legal if the victim is under another state's payment ban (essentially a mutual recognition of each other's prohibitions). Without something like that, a patchwork of laws could lead to forum-shopping—criminals might focus on subsidiaries in lenient jurisdictions or route communications to exploit gaps.

Coordination is also needed in the realm of incident reporting and information sharing. If multiple countries mandate rapid reporting of ransomware incidents (e.g., Australia's 72-hour rule, NIS2's 24-hour rule, US's upcoming 72-hour rule for certain sectors), then a victim might have to report to several regulators in different countries for one incident. This can be burdensome and, if not aligned, could cause confusion. Ideally, information shared with one country's CERT or law enforcement should be quickly relayed to others as needed. Mechanisms like the 24/7 Network of contact points under the Budapest Convention help ensure there is always a channel to share leads across borders in real-time [5]. International bodies like INTERPOL and Europol have also improved coordination by hosting joint ransomware task

forces. The more seamless the cross-border sharing of ransomware incident data, the more effectively authorities can connect the dots (e.g., linking ransom demands to known groups, or warning if a particular strain is spreading globally). This is a strong argument for harmonizing reporting requirements internationally—so that a company can, perhaps, make one comprehensive report that satisfies all jurisdictions, which are then shared among relevant agencies. It's also an argument for building something like a global database or at least regional databases of ransomware indicators (bitcoin wallet addresses, decryptor tools, etc.) accessible to law enforcement around the world.

Enforcement of a ransom payment ban itself is tricky across borders. If a company headquartered in Country X (ban in effect) secretly pays through an intermediary in Country Y (no ban), how will Country X catch and punish that? It might require cooperation from Country Y to trace the transaction. Financial regulations like anti-money laundering (AML) laws could help, as crypto exchanges are increasingly required to flag suspicious transfers. A strong international framework—perhaps leveraging the Financial Action Task Force (FATF) standards—could declare that ransom payments are a high-risk transaction type, prompting global financial institutions to report or block them. We already see steps in this direction with FATF's focus on virtual asset abuse and travel rule (which mandates info sharing on crypto transactions). If exchanges and banks worldwide start detecting ransom payments (often identified by certain on-chain patterns or known addresses) and alert authorities, that could backstop national bans.

In summary, cross-border cooperation is both the biggest challenge and the key to success in the fight against ransomware. National laws like bans or reporting mandates will have limited effect if ransomware operators can simply adapt by moving to jurisdictions where enforcement is weak. Conversely, if countries coordinate to make the world uniformly inhospitable to ransomware profits—through shared norms, synchronized laws, and joint enforcement—then the attackers' advantage of operating across borders can be curtailed. The current trajectory is promising in terms of awareness: numerous global forums and alliances are actively focused on ransomware in 2023–2025, more so than ever before. The task ahead is to translate that into concrete, harmonized action. The next section will consider the implications (positive and negative) of a broad move to ban ransom payments and whether an international treaty or agreement could fortify the global response.

4.3 Human rights and business implications of a ban

Policies around ransomware do not exist in a vacuum—they must be implemented in line with fundamental legal principles, including human rights, and with consideration of economic impacts on businesses. While at first glance banning ransom payments might seem purely a security measure, it can intersect with rights and business interests in subtle ways.

Human Rights Considerations: One area of concern is the potential impact on the rights to life, health, or security in cases where ransomware disrupts essential services. For instance, imagine a hospital's IT systems are locked by ransomware, halting vital medical equipment or access to patient records. If a strict law prohibits

paying the ransom under any circumstance, the hospital might remain crippled for days, directly endangering patients. Governments will need to consider whether exceptions or waivers for life-and-death situations are warranted. The U.S. White House discussion in 2023 explicitly floated a waiver for critical services: under the mooted policy, if a ransomware gang is *"preventing the delivery of critical services",* a victim could apply for a waiver to pay, with proper notification and permission from the government [10]. This acknowledges that a blanket ban could, in rare dire instances, conflict with the state's obligation to protect its citizens' lives and well-being. Thus, a nuanced ban might incorporate humanitarian exemptions (analogous to how some sanctions regimes allow exceptions for basic humanitarian needs). Another human rights angle is the right to privacy and data protection. In some ransomware cases, not paying leads attackers to publish or sell sensitive personal data (as part of "double extortion"). This can severely impact individuals' privacy and even safety (consider leaked medical or financial records). Victims might argue that they should be allowed to pay to protect individuals' privacy. However, legally mandating or allowing payment to safeguard privacy would set a problematic precedent; instead, robust data protection (encryption at rest, etc.) is the preferred solution. Policymakers must ensure that if companies are forbidden to pay, there are other measures to address the fallout for individuals—e.g., requiring companies to provide credit monitoring and support to persons whose data gets leaked because the company followed the law and didn't pay.

There is also the matter of due process and proportionality in penalizing victims. From a human rights perspective (especially under European human rights law), punishment should be proportionate and serve a legitimate aim. Punishing an organization (via fines or criminal liability) simply because it was a victim of a crime (ransomware) and attempted to mitigate damage by paying could be seen as harsh. Critics argue it's like *"victim-blaming"*—the law would be penalizing the injured party instead of just the perpetrator. To counter this, any ban would likely not impose criminal penalties on the act of payment for individuals (it could, for instance, impose fines on companies or administrative penalties, as the UK is considering). The UK's consultation even raised the idea of banning certain executives from serving on boards if they flout a payment prohibition [3], which is a severe sanction. If misapplied, that could raise concerns about fairness. Ensuring that companies have clear guidance, support from authorities, and perhaps some leniency in truly extenuating cases will be crucial so that a ransom payment ban doesn't inadvertently violate principles of fairness or put undue burden on victims in impossible situations. We should remember that human rights law (like the European Convention on Human Rights) does not explicitly protect the right of a company to transfer money to criminals, so banning payments isn't a direct human rights violation. But the *effects* of such a ban on other rights (life, security, property) need careful analysis. Property rights (e.g., the right to use one's money) can be restricted by law for public interest, so a ban would likely be upheld as lawful if properly legislated—much like anti-money-laundering laws are accepted—but authorities must enforce it in a proportionate manner.

Business and Economic Implications: For businesses, a legal ban on ransom payments marks a profound shift in risk management calculus. Currently, many

organizations view paying a ransom as an option of last resort—not desirable, but sometimes the least bad option to save the company. If that option is removed, companies may face higher costs in recovery and potentially greater losses from downtime or data loss. Small and medium enterprises (SMEs) are particularly vulnerable: they often lack the robust backups or redundant systems that larger firms have, and a ransomware attack could put them out of business if they cannot pay for a decryption key. As Kemba Walden highlighted, *"those [small organizations] can go bankrupt"* if a ban is in place and they suffer an attack unprepared [4]. This suggests that any payment ban should ideally be coupled with initiatives to support businesses in cybersecurity—e.g., government grants or insurance pools to help victims recover systems without paying criminals. The U.S. has started some programs (like grants for state and local government cybersecurity and exploring an incident response assistance fund), and the UK mentioned working with the insurance industry to provide better recovery support [3]. If businesses know they can't pay, they will need alternative lifelines: mutual aid agreements, data recovery vendors, public-private partnerships for incident response, etc. Over time, a ban could drive positive behavior changes in the private sector: companies might invest more in preventive security and robust backup systems, since they know paying ransom isn't an option. This could reduce the overall success rate of ransomware attacks (attackers frequently rely on victims lacking viable backups or business continuity plans).

However, in the short term, there could be economic disruption. Cyber insurers would have to adjust policies—many currently cover ransom payments; if those become illegal in some jurisdictions, insurers might instead offer more coverage for the costs of rebuilding networks or legal liabilities after an attack. Premiums might shift. It's possible some high-risk companies (like in healthcare) could find insurance more costly or scarce if they cannot resort to paying ransom to quickly resolve an incident. Some industry sectors might lobby against a ban, arguing it ties their hands. For instance, critical infrastructure operators might argue that a ban makes them sitting ducks if an attack threatens public safety and they legally cannot mitigate it via payment. On the flip side, companies that pride themselves on not paying (there are cases of firms that have public "no pay" policies) would welcome a ban as leveling the playing field—if nobody can pay, then those who currently refuse to pay (and possibly suffer more in the short term) won't be at a competitive disadvantage. It's somewhat analogous to how some companies wanted stricter environmental regulations so that all have to invest in compliance equally. Likewise, a ransom ban could remove the moral hazard where less-prepared companies know they can fall back on paying ransom or on insurance paying it. Moral hazard has been a real issue: readily paying ransoms arguably disincentivized some firms from investing in security or training. With a ban, that calculus changes; prevention becomes the only viable strategy.

There's also the broader economic impact: Ransomware payments amount to a huge transfer of wealth to criminal enterprises (an estimated $800+ million in 2024 alone) [47]. Stopping that flow could keep more money in the legitimate economy and avoid funding of other illicit activities (some ransomware gangs reinvest in other crimes or, in cases like North Korea's, fund weapons programs). But if a ban leads

to more data being destroyed or leaked, the losses might still manifest in other ways (like higher costs for remediation, lawsuits, or loss of customer trust). Businesses will have to contend with potential legal liabilities regardless: paying a ransom could violate data breach notification laws (since regulators may consider it concealment if not reported) or could violate sanctions; *not* paying and having data leaked could bring GDPR fines or other penalties if the incident resulted from poor security. So either route has costs. In a sense, a clear ban might simplify the decision—removing the agonizing choice and making it a legal certainty—but it also means the full brunt of recovery is on the victim.

One more implication: extortion dynamics might evolve. If attackers know payments are unlikely, they might change tactics. They could become more destructive out of spite (cyber vandalism) or pivot to purely data-centric extortion (stealing data and threatening leaks without encryption). We already see "harassment" techniques, like contacting a victim's clients or employees to exert pressure. A ban could reduce encryption-type attacks but increase other forms of digital extortion not easily addressed by a payment ban (like stealing embarrassing emails and asking for money not to leak them, which companies might classify differently). Legally, those are still extortion, but if the law focuses on "ransomware payments" it might not clearly cover payments to suppress leaked data, etc. Legislators might need to frame the law to cover extortion payments broadly, or criminals will exploit semantic loopholes (e.g., "this isn't a ransom for encryption, it's a consulting fee to 'delete' stolen data—is that banned?").

Overall, the business community's response to potential bans has been mixed. Surveys show theoretical support for bans, but when faced with real incidents, many businesses still consider payment as an option (hence the Yahoo Finance quip that *"everyone agrees ransomware payments should be banned until their own business gets hit"*). To make a ban workable, governments likely will engage in extensive outreach to companies, provide playbooks for response without paying, and maybe even legal safe harbors (immunity) for companies that come forward and don't pay, so they aren't unduly punished by regulators for the breach itself. This supportive ecosystem is crucial; otherwise companies might go bankrupt or attempt to hide incidents—outcomes beneficial to no one except the attackers.

In conclusion, a prohibition on ransom payments sits at the intersection of cybersecurity, law, and societal values. It seeks to prioritize long-term collective security (by removing criminal profit) potentially at the expense of short-term individual relief. Ensuring respect for fundamental rights and mitigating harm to businesses will require careful legal drafting (with exceptions, if needed) and robust support measures. Done properly, it could shift norms—making it as unthinkable to pay a cyber-ransom as it is now to pay a kidnapping ransom to terrorists, a comparison often drawn. But done hastily or without support, it could cause significant collateral damage among the very victims it aims to protect.

5 Toward an international framework for ransomware

Given the global nature of ransomware, many experts argue that isolated national efforts, while helpful, are not sufficient. What might an international treaty or coordinated framework to address ransomware look like, and how could it improve upon the patchwork of responses currently emerging? In this final section, we discuss possible elements of a global strategy and weigh the prospects of an international agreement specifically targeting ransomware.

1. Coordinating Legal Prohibitions and Reporting Requirements: One straightforward step would be for like-minded countries to harmonize their laws on ransom payments. This could be done via a formal agreement or simply parallel legislation. For instance, a group of countries (perhaps through the CRI or G7) could jointly declare that they will ban ransom payments by certain entities (government agencies, critical infrastructure, etc.) and require prompt reporting of all ransomware incidents and payments. If done in unison, this reduces the risk that criminals will play jurisdictions against each other. An international framework could provide a model law or standards that each nation domestically implements—similar to how the FATF provides model regulations for money laundering which members adopt. Even without a binding treaty, a coordinated announcement (like CRI's joint statement for governments not paying) [6] sends a powerful message to both criminals and the private sector. Over time, one could envision a multilateral agreement where parties agree to outlaw ransom payments to cybercriminals, perhaps with an article allowing urgent exceptions (like life-threatening situations) and with commitments to share information about incidents.
2. Enhanced International Law Enforcement Cooperation: A treaty or framework should bolster the operational side of fighting ransomware. This includes faster extradition processes for ransomware suspects, joint investigations, and asset freezing across borders. The proposed UN cybercrime convention is expected to include provisions for mutual legal assistance and extradition for cyber offenses, which would cover ransomware. To specifically target ransomware, the convention (or a protocol) could designate ransomware extortion as an offense for which extradition should be granted (with no refusal on political grounds, etc.). Additionally, an international framework might establish multinational task forces that pool expertise and simultaneously execute coordinated actions (raids, server seizures) in multiple countries. Operation Cronos against LockBit, cited by Chainalysis, was one example where an "international coalition" seized infrastructure in a concerted strike [47]. Institutionalizing such cooperation via an agreement—for example, committing resources to permanent joint ransomware investigative units—could make law enforcement more nimble than the criminals.

Another aspect is addressing cryptocurrency tracing and abuse on a global scale. Ransomware's rise has been facilitated by the pseudonymous nature of cryptocurrency. A global framework could push for unified know-your-customer (KYC) rules for crypto exchanges (so attackers have fewer outlets to cash out) and encourage countries to share blockchain analytics data. In 2023, the Counter Ransomware Ini-

tiative launched an anti-virtual asset misuse working group, which is a start [6]. A treaty might not detail crypto policy, but it could mandate cooperation in tracing and seizing cryptocurrency proceeds of ransomware, treating them akin to proceeds of drug trafficking under the UN Convention Against Transnational Organized Crime. One could imagine an international capability to quickly freeze or blacklist crypto addresses associated with major ransomware attacks, so the criminals cannot easily collect or move the funds.

3. International Support Mechanisms for Victims: If payments are to be banned, an international framework might include creating safety nets for victims. One idea floated in policy circles is an international ransomware recovery fund—financed perhaps by contributions from governments or industry—that could aid victims in restoring systems and data in lieu of paying a ransom. This would mirror how some countries have victim compensation funds for terror attacks or violent crimes. While it might seem unlikely for governments to effectively insure private companies against cyber losses, a collective fund could be targeted at critical sectors or smaller businesses who lack resources. By helping victims recover without paying criminals, such a mechanism would reinforce the no-payment policy. An international agreement could encourage states to establish national funds or to contribute to a cross-border pool for emergency cyber assistance. Additionally, an international framework could facilitate the sharing of decryption keys and tools. There is already the "No More Ransom" initiative (a collaboration between Europol and cybersecurity companies) which provides free decryptors for known ransomware strains; a treaty could formally endorse and expand such efforts, making it an obligation for law enforcement agencies to share any recovered keys or techniques for decryption with a central repository.
4. Addressing Safe Havens and State Responsibility: A tougher element is how to handle states that harbor ransomware gangs. International law could evolve to impose consequences on nations that systematically refuse to cooperate against ransomware. This is tricky—attributing responsibility to a state for non-state hacker groups is diplomatically sensitive. However, a strong international stance might be to incorporate ransomware into discussions of state responsibility for cybercrime. For example, the framework could assert that countries must not knowingly allow their territory to be used for internationally wrongful acts (building on existing norms that a state should not allow its territory to be a haven for cyberattacks). If a country consistently protects ransomware actors, others might consider sanctions or even countermeasures. Indeed, in 2022 the United States publicly attributed certain ransomware to actors in safe havens and hinted at using offensive cyber operations to disrupt them if cooperation isn't forthcoming. An international accord could explicitly or implicitly bless collective measures against major ransomware infrastructures (like botnets) that are headquartered in uncooperative jurisdictions—somewhat akin to how naval powers historically cooperated to combat piracy in lawless regions.
5. Treaty vs. Soft Law: Would a dedicated "Ransomware Treaty" be viable or even necessary? Perhaps not as a standalone; ransomware is part of the broader cybercrime landscape. It might be more realistic to integrate ransomware-specific pro-

visions into existing frameworks. The UN Cybercrime Convention could be one vehicle; or the Council of Europe could add a Third Protocol to the Budapest Convention specifically about emerging cybercrime issues like ransomware and financial extortion. Another route is a political agreement—e.g., a G7 agreement or an OECD guideline—that isn't legally binding but sets best practices that many nations adopt domestically. The advantage of a treaty is binding commitments and a clear signal, but negotiating a new treaty (or amendments) can take years. Meanwhile, ransomware is a crisis now. Thus, a coordinated framework short of a treaty might emerge: essentially, alignment of domestic laws and cooperation through networks like CRI and Interpol, without a single new global legal instrument. Over time, if that proves insufficient or if there is broad consensus (excluding a few rogue states), a treaty could formalize the norms.

Pros and Cons of an International Ban: If hypothetically a critical mass of countries agreed to ban ransom payments, the potential benefits would be significant: The financial incentive for ransomware could collapse if attackers know that in all major economies, victims are legally barred from paying. Ransomware groups would struggle to make money, which could lead many to disband or switch to other crimes. We have some precedent in the data: as noted, the volume of payments fell in 2024 as more victims refused to pay, and that directly hurt ransomware revenues [47]. A coordinated ban could amplify this effect dramatically. Furthermore, it would eliminate the moral hazard problem internationally—companies everywhere would have to up their security game, and none could undercut others by quietly paying. An international ban could also simplify messaging: a clear global norm of "we do not negotiate with cyber-hostage takers" might deter some would-be criminals and strengthen public-private trust (companies won't feel pressured to pay if they know it's illegal and socially disapproved, and they can instead turn to law enforcement for help).

However, the cons on an international scale mirror those at national level, but with additional complexity. If not every country joins the ban, ransomware actors will focus on victims in countries where payment is still an option, potentially concentrating damage there. If, say, NATO and allies ban payments but some large emerging economies do not, attackers might refocus on the latter—which could create political friction (those countries may feel they are now bearing the brunt of attacks "diverted" from the West). So achieving near-universal adherence would be important to avoid simply shifting the problem. Another con is enforcement disparity: even if many countries sign on, will all enforce the ban equally? Countries with less cyber investigative capacity might struggle to detect if companies pay illicitly. This could create weak links exploited by criminals. It could also create trade or competition issues: what if a multinational company in Country A (ban in place) loses out to a competitor in Country B (ban not enforced) after a ransomware incident because the competitor secretly paid and recovered faster? Such scenarios could cause tension unless there is uniform commitment. Additionally, at an international law level, making ransom payment illegal globally could push the activity into black markets—for example, we might see the rise of covert negotiation firms that operate

from non-treaty countries facilitating payments under the radar, complicating law enforcement.

Human rights and Internet freedom implications globally: There's an opposite concern some human rights advocates have: that authoritarian regimes might co-opt anti-ransomware laws to justify monitoring or restricting internet use. For instance, a government could pass a broad law claiming to target ransomware payments but then use it to surveil cryptocurrency transactions of dissidents or penalize NGOs under the guise of "potential ransom transactions". The UN treaty negotiations saw worries that vague cybercrime laws might be misused this way [9]. Drafters of international principles should thus ensure clarity—focusing on actual ransomware scenarios—and encourage safeguards like judicial oversight for any enforcement actions, to avoid abuse.

In sum, an international treaty or framework addressing ransomware would likely focus on prevention (reducing targets and vulnerabilities), enforcement (increasing the risk to attackers), and ideational change (making paying ransoms socially and legally unacceptable). We already see elements of this in collaborative efforts like the CRI and joint law enforcement operations. The logical progression is tighter alignment of laws and possibly a formal pact. Whether through a treaty or coordinated national laws, the pros include starving ransomware gangs of revenue, fostering global unity against a common enemy, and pooling resources/knowledge for defense. The cons and challenges include getting broad buy-in, avoiding negative consequences for victims during the transition, and dealing with holdout states and non-state complexities.

6 Conclusion

Ransomware's rise to infamy as a global scourge has compelled jurists and policymakers to rethink traditional cybercrime strategies. In exploring the question, "Toward a ban on payments?", we find a landscape in 2023–2025 that is rapidly evolving. The United States has not outlawed ransom payments, but discussions at the highest levels signal that the idea is on the table, pending improvements in cyber resilience [4]. In the meantime, the U.S. is tightening the screws via mandatory reporting (CIRCIA) and sanctions enforcement, effectively discouraging payments to certain actors [18]. The United Kingdom is on the cusp of implementing one of the most aggressive anti-ransomware legal regimes yet, combining a targeted payment ban for critical sectors with a novel payment oversight and reporting system. Across the European Union, the focus is on transparency (with NIS2's reporting mandates) and on coordination through existing legal tools, while individual states voice growing openness to stronger measures. Australia has already implemented a pioneering law to force disclosure of ransom payments within 72 h, reflecting a belief that shining light on the problem will help curtail it [6].

These efforts, while promising, also underscore the challenges. A patchwork of laws can create loopholes; overly draconian rules can backfire if not coupled with support. The debate reveals legitimate concerns: Will banning payments protect long-term public interest at the cost of short-term harm to some victims? How

do we ensure that not paying ransoms indeed leads to fewer attacks, rather than simply more damages from uncompensated attacks? The evidence to date suggests that reducing ransom payments does, in fact, undermine the ransomware business model—the marked drop in total ransomware revenue in 2024 is attributed partly to more victims refusing to pay and more concerted law enforcement action [47]. In theory, if no one paid, most ransomware groups would eventually disband for lack of profit. The key is managing the interim period and preventing solitary defections (one victim paying can sustain an attacker even if others do not).

International law provides a critical framework for this fight. Existing cybercrime treaties like the Budapest Convention give countries the legal basis to pursue and cooperate against ransomware perpetrators [5]. Emerging instruments like the UN Cybercrime Convention aim to bring all nations on board, closing jurisdictional gaps [9]. These conventions, along with soft-law norms from bodies like the UN Security Council (in analogous contexts) and coalitions like the CRI, are forging a global norm that tolerating cyber extortion is not acceptable. The trajectory is reminiscent of how the world gradually agreed that paying terrorists is inadvisable [46]—we may be witnessing the early stages of a similar consensus for ransomware. Notably, the CRI's pledge that governments won't pay ransoms is a significant normative milestone [6]. If extended to industry via national laws, this could standardize expectations.

From a legal efficacy standpoint, one cannot ignore the necessity of tackling ransomware's root enablers: the anonymity of cryptocurrency and the sanctuary provided by certain states. Legal responses to ransom payments must thus be part of a comprehensive strategy: vigorous prosecution of cybercriminals (utilizing international cooperation), financial sanctions and anti-money-laundering measures to make extortion proceeds harder to use, and robust requirements for organizations to harden their defenses and promptly report attacks. A ban on payments, in isolation, is not a silver bullet—but as one tool among many, it could significantly tilt the cost-benefit calculus against the attackers.

It is also a legally intriguing tool: criminalizing an act (ransom payment) that is itself a byproduct of another crime forces a re-examination of victim's role in cybercrime. Traditionally, victims are not penalized; here, some argue it's necessary to do so (lightly, via fines or restrictions) to prevent greater harm. If done, it must be approached carefully, with clear legal standards and perhaps a phased implementation allowing organizations to reach a baseline of preparedness. International human rights law does not forbid such measures, but fairness and proportionality must guide enforcement. Courts may eventually be called to consider cases where, for example, a company paid a ransom to save lives in defiance of a ban—one hopes laws will be written with enough flexibility to accommodate truly extenuating circumstances so that just outcomes prevail.

Looking ahead, the prospect of an international treaty or formal framework specifically on ransomware is no longer far-fetched. Whether through an additional protocol, a UN resolution, or a standalone agreement, the elements are coming into focus: universal criminalization of ransomware offenses; commitment to not pay or facilitate ransoms; obligation to share incident information; collaborative disruption of ransomware infrastructure; and assistance to victims. The pros and cons we analyzed suggest that while a universal ban on payments might be the end goal, intermediate

steps are needed—essentially a global "road map" to get there, as referenced by experts like Walden and Stifel [4]. That means building resilience and alternatives so that when the revenue tap to criminals is turned off, we do not inadvertently punish ourselves more than the enemy.

In conclusion, international legal responses to ransomware are visibly coalescing around a more hard-line stance: diminishing or even outlawing ransom payments is on the policy menu in multiple jurisdictions and forums. This represents a bold evolution in cybersecurity law—shifting from purely defensive or reactive postures to an offensive strategy of starving attackers of their profits. While significant hurdles remain, the direction is set toward greater international coordination. If nations can align their laws and cooperate fully, ransomware's heyday may eventually recede, much as other forms of organized crime have been curbed when the world acted in concert. The epidemic of ransomware will not be cured overnight, but through steady legal pressure—bans, transparency, and global teamwork—we may finally be able to say that paying a ransom is not just inadvisable, but a relic of a less secure past.

Conflict of interest F. Teichmann declares that he/she has no competing interests.

References

1. Allnutt H, Hill P Prevention, reporting, payments: UK government consults on ransomware. Lexology. https://www.lexology.com/library/detail.aspx?g=e5704df2-488d-4182-9681-4fdbf772f0a2. Accessed 4 Sept 2025
2. Aw C, Buti P (2025) Australia mandates first-of-kind reporting of ransomware payments. Hogan Lovells. https://www.hoganlovells.com/en/publications/australia-mandates-firstofitskind-reporting-of-ransomware-payments. Accessed 4 Sept 2025
3. Blest A, Scali G From target to fortress: UK's new ransomware payment ban proposal explained, Lexology. https://www.lexology.com/library/detail.aspx?g=d265782c-6798-414f-81f2-0750c1455573. Accessed 4 Sept 2025
4. Bracken M (2024) Ex-white house cyber official says ransomware payment ban is a ways off. Cyberscoop. https://cyberscoop.com/ex-white-house-kemba-walden-ransomware-payment-ban. Accessed 4 Sept 2025
5. Council of Europe (2022) News—Ransomware: new guidance note by the T-CY. Council of europe. https://www.coe.int/en/web/cybercrime/-/ransomware-new-guidance-note-by-the-t-cy. Accessed 4 Sept 2025
6. Crowell (2025) Targeted policy action against ransomware attacks emerging as a key global cybersecurity trend. Crowell. https://www.crowell.com/en/insights/client-alerts/targeted-policy-action-against-ransomware-attacks-emerging-as-a-key-global-cybersecurity-trend. Accessed 4 Sept 2025
7. Dalton P, Moir A, Tirmizi A (2025) UK government looks set to introduce ransomware payment ban and mandatory reporting. Herbert smith Freehills Kramer. https://www.hsfkramer.com/

notes/cybersecurity/2025-posts/uk-government-looks-set-to-introduce-ransomware-payment-ban-and-mandatory-reporting. Accessed 4 Sept 2025
8. Hutchison E (2021) Should ransomware payment be illegal in Canada? Cira. https://www.cira.ca/en/resources/news/cybersecurity/should-ransomware-payments-be-illegal-canada. Accessed 4 Sept 2025
9. Jones D (2024) US hopes to leverage UN cybercrime treaty toward ransomware fight. Cybersecurity dive. https://www.cybersecuritydive.com/news/biden-administration-un-cybercrime-treaty/732643. Accessed 4 Sept 2025
10. Kapko M (2023) White house considers ban on ransom payments, with caveats. Industry dive. https://www.cybersecuritydive.com/news/white-house-considers-ransom-payment-ban/649673/. Accessed 4 Sept 2025
11. Leiu A UK government moves to ban ransomware payments for public sector. Lexology. https://www.lexology.com/library/detail.aspx?g=bc748226-c89b-499d-8bca-b3079fb6030f. Accessed 4 Sept 2025
12. Locke PT (2024a) Restrictions on paying a ransom demand. Troutman pepper Locke. https://www.consumerfinancialserviceslawmonitor.com/2024/07/restrictions-on-paying-a-ransom-demand/. Accessed 4 Sept 2025
13. Locke PT (2024b) Restrictions on paying a ransom demand—dear Mary—incidents + investigations Cybersecurity advice column. https://www.jdsupra.com/legalnews/restrictions-on-paying-a-ransom-demand-9910688. Accessed 4 Sept 2025
14. Machin E Held to ransom? UK consult on industry-wide payment approval regime. Lexology. https://www.lexology.com/library/detail.aspx?g=30598c2c-a66c-47c3-bae5-9747b43b1c90. Accessed 4 Sept 2025
15. Morgan S (2024) Boardroom Cybersecurity report 2024. Secureworks. https://www.secureworks.com/centers/boardroom-cybersecurity-report-2024. Accessed 4 Sept 2025
16. Public Safety Canada (2023) Parliamentary committee notes: Ransomware. Public safety Canada. https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240614/18-en.aspx. Accessed 4 Sept 2025
17. Randall PK (2022) Two states prohibit entities from paying ransoms. Conell Foley. https://www.connellfoley.com/blog/Two-States-Prohibit-Public-Entities-Paying-Ransoms. Accessed 4 Sept 2025
18. Ribeiro A (2021) CRS report examines ransomware and federal law, in the era of rising cybercrime and cybersecurity attacks. Industrial Cyber. https://industrialcyber.co/threats-attacks/crs-report-examines-ransomware-and-federal-law-in-the-era-of-rising-cybercrime-and-cybersecurity-attacks. Accessed 4 Sept 2025
19. Tag Alliances (2024) Mandatory reporting of ransomware payments may soon be law. What you need to know. Tag alliances. https://www.tagalliances.com/specialty-groups/ip-it-cyber-security/15005-mandatory-reporting-of-ransomware-payments-may-soon-be-law-what-you-need-to-know. Accessed 4 Sept 2025
20. Teichmann F (2017) Twelve methods of money laundering. J Money Laund Control 20(2):130–137. https://doi.org/10.1108/JMLC-05-2016-0018
21. Teichmann F (2018) Financing terrorism through cryptocurrencies—a danger for Europe? J Money Laund Control 21(4):513–519. https://doi.org/10.1108/JMLC-06-2017-0024
22. Teichmann F (2019a) European antiquities trade: a refuge for money laundering and terrorism financing. J Money Laund Control 22(3):410–416. https://doi.org/10.1108/JMLC-09-2017-0051
23. Teichmann F (2019b) Financing of terrorism through the banking system. J Money Laund Control 22(2):188–194. https://doi.org/10.1108/JMLC-07-2017-0026
24. Teichmann F (2019c) Money laundering and terrorism financing through consulting companies. J Money Laund Control 22(1):32–37. https://doi.org/10.1108/JMLC-10-2017-0056
25. Teichmann F (2019d) Recent trends in money laundering and terrorism financing. J Financial Regul Compliance 27(1):2–12. https://doi.org/10.1108/JFRC-03-2018-0042
26. Teichmann F (2020a) Money-laundering and terrorism-financing compliance—unsolved issues. J Money Laund Control 23(1):90–95. https://doi.org/10.1108/JMLC-02-2018-0014
27. Teichmann F (2020b) Money laundering in the jewellery business. J Money Laund Control 23(3):691–697. https://doi.org/10.1108/JMLC-03-2018-0020
28. Teichmann F (2020c) Recent trends in money laundering. Crime Law Soc Chang 73(2):237–247. https://doi.org/10.1007/s10611-019-09859-0
29. Teichmann F, Falker C (2020a) Money laundering through banks in Dubai. J Financial Regul Compliance 28(3):337–352. https://doi.org/10.1108/JFRC-07-2019-0087
30. Teichmann F, Falker C (2020b) Money laundering through cryptocurrencies. In: 13th international scientific and practical conference—artificial intelligence Anthropogenic nature vs. Social origin:500–511. Springer, https://doi.org/10.1007/978-3-030-39319-9_57

31. Teichmann F, Falker C (2020c) Money laundering through deposit boxes. J Money Laund Control 23(4):805–818. https://doi.org/10.1108/JMLC-07-2019-0058
32. Teichmann F, Falker C (2021a) Money laundering via cryptocurrencies—potential solutions from Liechtenstein. J Money Laund Control 24(1):91–101. https://doi.org/10.1108/JMLC-04-2020-0041
33. Teichmann F, Falker C (2021b) Money laundering via underground currency exchange networks. J Financial Regul Compliance 29(1):1–14. https://doi.org/10.1108/JMLC-07-2019-0060
34. Teichmann F (2023a) Current developments in money laundering and terrorism financing. J Money Laund Control 26(2):337–348. https://doi.org/10.1108/JMLC-05-2019-0043
35. Teichmann F (2023b) Ransomware attacks in the context of generative artificial intelligence—an experimental study. Int Cybersecur Law Rev 4(4):399–414. https://doi.org/10.1108/JMLC-10-2017-0056
36. Teichmann F, Falker C (2023) Money laundering—the gold method. J Money Laund Control 26(3):509–522. https://doi.org/10.1108/JMLC-07-2019-0060
37. Teichmann F, Wittmann C (2023a) Money laundering in the United Arab Emirates: the risks and the reality. J Money Laund Control 26(4):709–718. https://doi.org/10.1108/JMLC-01-2022-0014
38. Teichmann F, Wittmann C (2023b) When is a law firm liable for a data breach? An exploration into the legal liability of ransomware and cybersecurity. JFC 30(6):1491–1498. https://doi.org/10.1108/JFC-04-2022-0093
39. Teichmann F, Boticiu R, Sergi S (2023) The evolution of ransomware attacks in light of recent cyber threats. How can geopolitical conflicts influence the cyber climate? Int Cybersecur Law Rev 4(3):259–280. https://doi.org/10.1365/s43439-023-00095-w
40. Teichmann F, Boticu S (2024a) How do cybercriminals launder the proceeds of their crimes? Int Cybersecur Law Rev 5(1):67–77. https://doi.org/10.1365/s43439-023-00104-y
41. Teichmann F, Boticiu R (2024b) The most impactful ransomware attacks in 2023 and their business implications. Int Cybersecur Law Rev 5(2):301–311. https://doi.org/10.1365/s43439-024-00115-3
42. Teichmann F, Boticiu S (2024c) How does one negotiate with ransomware attackers? Int Cybersecur Law Rev 5(1):55–65. https://doi.org/10.1365/s43439-023-00106-w
43. Teichmann F, Boticiu R, Sergi S (2024) Compliance issues in arbitration proceedings—bribery, money laundering and other abuses. JFC 31(3):759–767. https://doi.org/10.1108/JFC-10-2022-0241
44. Teichmann F (2025a) Cybersecurity of critical infrastructure in europe: the NIS2 directive in focus. Int Cybersecur Law Rev 6(3):207–220. https://doi.org/10.1365/s43439-025-00154-4
45. Teichmann F (2025b) Ransomware extortion in europe: legal responses and mitigation strategies. Int Cybersecur Law Rev. https://doi.org/10.1365/s43439-025-00152-6
46. United Nations (2014) Security council adopts resolution 2133 (2014), calling upon states to keep ransom payments, political concessions from benefiting terrorist. United nations. https://press.un.org/en/2014/sc11262.doc.htm. Accessed 4 Sept 2025
47. Wright R (2025) Ransomware payments fell 35% in 2024. Cybersecurity Dive. https://www.cybersecuritydive.com/news/ransomware-payments-fell-35-in-2024/739298. Accessed 4 Sept 2025