Global Cybercrime Requires a Collective Response

Are We Prepared to Ban Ransom Payments?

Roberto Baldoni | National Cybersecurity Agency of Italy

The ransomware industry can be effectively countered only by banning ransom payments, which requires technical, normative and investigation alignment across countries. A specialized international organization, based on a public–private partnership, should coordinate the effort by supporting affiliated countries in filling gaps.

Since 2019, following the creation of the first website exposing data stolen in ransomware attacks, over 80 cybercriminal groups have adopted a sophisticated extortion model based on three distinct phases, resulting in staggering cryptocurrency turnovers reaching several billion U.S. dollars. No country, regardless of its wealth, is immune to these attacks. Cybercriminals have recently managed to cripple the operations of entire medium-sized countries like Costa Rica and Montenegro, as well as large-scale infrastructure such as the Colonial Pipeline in the United States, causing weeks-long disruptions in fuel distribution on the East Coast. Italy endured an attack on its major railway operator, leading to several days of inconveniences that affected millions of commuters and long-distance passengers. Moreover, criminal crews sometimes act as arms of more sophisticated attacks orchestrated by state actors.[1] All of this makes fighting and dismantling such crews a priority for the international community.

©SHUTTERSTOCK.COM/NUTZ

Between 2020 and 2022, there have been almost 7,000 documented ransom demands on these platforms globally, but this is merely the visible portion of a much larger problem. Most ransomware incidents remain hidden because victims opt to pay during the initial stages of extortion. Victims choose immediate payment due to the exorbitant daily cost of downtime resulting from system lockouts, anticipating further costs in subsequent phases, in addition to an escalating ransom demand. A recent study of Australian CEOs of medium to large companies reveals that nearly three-quarters (74%) of executives who experienced an attack chose to pay the ransom within 48 h. Of those, nearly 37% paid within 24 h.[2]

In the second phase, the criminal group tarnishes the victim's reputation by announcing the attack on their website. If the victim still refuses to pay, the third phase of extortion commences with the public release of a sample of stolen data, offered for sale to the highest bidder. This not only jeopardizes the victim's competitiveness as rivals gain access to their strategic data but also exposes them to potential privacy violation lawsuits. A recent report by IBM estimates the average cost to the company to

Digital Object Identifier 10.1109/MSEC.2024.3401289
Date of current version: 17 July 2024

recover operations from a ransomware attack at US$4.5 million.[3] If the ransom is not paid, it may take months to restore full operation, but even if it is paid, there is no guarantee that full operation will be restored in a short time. Moreover, the criminal gang that has complete control over the victim's computer systems might leave back doors for future intrusions.

It is crucial that organizations employ all techniques to protect the attack surface, cultivate collective awareness through adequate cybersecurity training for employees (recent data show that 68% of data breaches are due to human errors),[4] and prepare to resume operations postattack. However, the ransomware scourge can only be defeated by drastically reducing the flow of money through banning ransom payments. While this ethical and legal issue has been widely debated in every developed country, none has yet taken concrete measures, because the issue is controversial. Banning ransom payments offers distinct advantages. It enables early detection of extortion, enhancing the ability to combat this threat effectively. Victims are discouraged from paying because doing so may expose them to double extortion as attackers might threaten to reveal their payments. Most importantly, it reduces illegal fund flows, making this activity less profitable and consequently less attractive and innovative. To draw a parallel, the historic U.S. "no-concessions" policy for negotiating with terrorists who abduct hostages is defended on the basis that paying ransoms finances terrorist groups. While for many terrorist groups like ISIS, kidnapping is only a minor source of revenue,[5] in the case of ransomware, criminal revenues are reinvested and become fuel for the expansion of the business. Thus, the "no-concessions" policy is a primary tool to curb this threat and keep it negligible.

Most importantly, it reduces illegal fund flows, making this activity less profitable and consequently less attractive and innovative.

Nonetheless, a "no-concessions" policy in cyberspace has drawbacks as affected companies might disrupt supply chain operations and suffer financial crises with possible ripple effects on customers and suppliers. Moreover, a ban from a single nation would not work, as large companies could still make payments through an overseas branch or offshore bank accounts. Meanwhile, it would expose local small and medium-sized enterprises, public administrations, and hospitals to the risk of business collapse.

To defeat a plague that exploits global platforms, the ban should be embraced "at scale" by as many nations as possible, resulting in the largest possible public–private response. In recent years, collaborative efforts among law enforcement authorities of different countries have led to the takedown of some major criminal crews (mainly centered in the Five Eyes countries). Additionally, significant progress has been made to help victims resume operations, improve traceability in cryptocurrency exchanges, and enhance the anti-money-laundering system.

So, the pivotal question is, Are we ready to take a strong, unified stance among a wide number of nations to outlaw ransom payments, drawing a distinct line between legality and illegality? To quickly reach the moment when the answer to this question is a solid yes, such countries should align "at scale" with many normative aspects to enable quick coordination in investigations, penalties on individuals associated with ransomware groups (including lengthy imprisonment and asset freezes), and information sharing.

In addition to law enforcement actions, there is a need to work on resilience in each nation for prevention, just as with any other public infrastructure. To reduce the number of car accidents, drivers need to have valid licenses, car manufacturers should build safer vehicles, and road builders must keep the roads safe by repairing dangerous potholes and installing guardrails along the edge of the road. After an accident, the degree of liability among parties is evaluated. The same principles apply to the much more intricate cybersecurity scenarios. CEOs and boards of the victim should be held accountable for neglecting to implement preventive cybersecurity best practices, while software providers and integrators should be responsible for failing to address critical security problems in their software products and systems. The degree of liability should be proportional to the type of negligence, consider the complexities of the software supply chain, and recognize that not all cyberattacks can be prevented even if an organization applies cybersecurity best practices. Additionally, not all vulnerabilities can be detected and fixed, even with best-in-class secure software development tools. Implementing such measures would yield a dual benefit: enhancing the resilience of software products, services, and organizations against cyberattacks and encouraging software development companies to compete on the security of their software, as pursued by the Biden administration.

Moreover, banning ransom payments requires careful articulation to strike delicate balances. This includes handling exceptions to the ban if the damage could exceed an acceptable social threshold. This means that some local organizations should have the legal right to set exceptions, and such exceptions should follow internationally agreed guidelines. This is not new, as many countries handle exceptions to rigorous "no-concessions" policies toward terrorists who have abducted hostages.[5] The United States, for instance, established the Hostage Recovery Fusion Cell in 2015 to coordinate hostage recovery operations across the U.S. government, opening the door to private ransom payments. Such exceptions could create room for the establishment of a cybersecurity insurance market that will incentivize insurers' customers to take adequate preventive measures, guide interactions with the cybercriminal underworld, and support full recovery of operations. This contributes to improving customers' cyber resilience. Similar principles were applied to minimize the risk of kidnapping workers in dangerous places through worker insurance.[6]

It is obvious that such a degree of strict alignment and coordination among nations cannot be left to important but loosely coupled multilateral diplomatic international cooperation. There is a need for tight operational alignment in legislation, investigation, justice, and resilience. INTERPOL serves as an example of an instrument for operational alignment in investigations. The Counter Ransomware Initiative (CRI), started in 2021, is without a doubt the most advanced international exercise in this direction, bringing together cybersecurity officials from over 50 countries and major private companies to holistically address the scourge. CRI strengthens international cooperation through several coordinated efforts, such as joint operation meetings, information and intelligence sharing, law enforcement collaboration, diplomatic engagement (to encourage noncooperative countries to crack down on ransomware groups operating within their borders), public–private partnerships, capacity building, and technical assistance.

However, considering the number and scale of engagements, for this cooperation to be effective and timely, it cannot be relegated to the leftover time of national cybersecurity agencies, which are completely busy with their domestic cyber issues. The question could therefore become, Do we need an international organization whose specific mission is to keep advancing nations' alignment on the several fronts identified by the CRI, to more quickly reach the point of banning ransom payments, and to collectively face future cybercrime challenges?

This is a complex international undertaking whose primary mission is to facilitate and accelerate trusted, timely, and continuous collaboration among affiliated countries and the private sector.[1] The perimeter of this collaboration will depend on geopolitical conditions; the larger the perimeter, the more effective the fight against cybercrime will be.

Every day delayed in commencing this lengthy path increases the risk of drawing the most talented hackers, who are already in short supply, toward criminal groups. They may be tempted by the substantial and rapid profits, and their decision is also facilitated by the current overly permissive and nationally fragmented legal system, full of gray areas and small, slow, or nonexistent reactions at the international level. If the dark side of the Force gains ground by drawing in the best talents, the battle against cybercrime will be more challenging than ever. ■

References

1. R. Baldoni, *Charting Digital Sovereignty: A Survival Playbook*. Seattle, WA, USA: Amazon, 2024.
2. D. Hopkins, B. Sutton, and B. Pane, "Ransomware: A cost of doing business?" McGrathNicol, Melbourne, Australia, 2023. [Online]. Available: https://www.mcgrathnicol.com/insight/ransomware-a-cost-of-doing-business/
3. "Cost of a data breach report 2023," IBM Security, Armonk, NY, USA, 2023. [Online]. Available: https://www.ibm.com/reports/data-breach
4. "Data breach investigations report," Verizon, New York, NY, USA, 2024. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/
5. C. Mellon, P. Bergen, and D. Sterman, "To pay ransom or not to pay ransom? An examination of western hostage policies," New America, Washington, DC, USA, 2017. [Online]. Available: https://www.newamerica.org/future-security/policy-papers/pay-ransom-or-not/
6. A. Shortland, "Governing criminal markets: The role of private insurers in kidnap for ransom," *Governance*, vol. 31, no. 2, pp. 341–358, 2018, doi: 10.1111/gove.12290.

Roberto Baldoni is a central director at the National Cybersecurity Agency of Italy, 00187 Rome, Italy and an honorary professor if computer science at Sapienza University of Rome. His research interests include digital sovereignty and geopolitics and governance of technology. Contact him at r.baldoni@acn.gov.it.