UNODC
United Nations Office on Drugs and Crime

RANSOMWARE
POLICY PAPER

UNITED NATIONS OFFICE ON DRUGS AND CRIME

Ransomware policy paper

UNITED NATIONS
Vienna, 2023

Acknowledgements

The United Nations Office on Drugs and Crime (UNODC) would like to express its gratitude to two experts who provided in-kind assistance at all three expert group meetings. Special thanks go to Vijay Rathour, partner and Head of the Digital Forensics Group at Grant Thornton, and Samir Aliyev, Director of Cyber Security and Data Protection Programmes at the University of St. Gallen in Switzerland.

The present policy paper was prepared by the Strategy, Planning and Field Support Unit, Cybercrime and Anti-Money-Laundering Section, Division for Treaty Affairs, UNODC, under the supervision of Glen Prichard, Chief of the Cybercrime and Anti-Money-Laundering Section.

UNODC acknowledges the financial contribution of the Government of the United States of America for this report.

Drafting

Alyaksandr Malyshau

Review and comments

Michiel van Dyk

Nayelly Loya Marin

Renata Delgado-Schenk

Jonathan Fishman

© United Nations Office on Drugs and Crime, 2023.

The designations employed and the presentation of material in this publication do not imply the expression of any opinion whatsoever on the part of the Secretariat of the United Nations concerning the legal status of any country, territory, city or area, or of its authorities, or concerning the delimitation of its frontiers or boundaries.

Information on uniform resource locators and links to Internet sites contained in the present publication are provided for the convenience of the reader and are correct at the time of issue. The United Nations takes no responsibility for the continued accuracy of that information or for the content of any external website.

Publishing production: English, Publishing and Library Section, United Nations Office at Vienna.

Cover images: © Maksim Kabakou/stock.adobe.com, releon8211/stock.adobe.com

Contents

LIST OF FIGURES

Executive summary

The present threat analysis and policy paper summarizes the results of three expert group meetings, held in East and Southern Africa, Latin America and the Caribbean and the Asia-Pacific region in 2022. Based on the most recent research and literature, the paper provides practical approaches for policymakers to consider in managing or preparing for ransomware incidents.

The three expert group meetings were attended by experts from academia and the private sector and by representatives from 10 countries in East and Southern Africa (Botswana, Kenya, Malawi, Mauritius, Namibia, Seychelles, South Africa, Uganda, United Republic of Tanzania and Zambia), 9 countries in South and Central America (Argentina, Belize, Colombia, Costa Rica, Dominican Republic, Mexico, Panama, Paraguay and Peru) and 11 countries in the Asia-Pacific region (Cook Islands, Fiji, Indonesia, Lao People's Democratic Republic, Malaysia, Papua New Guinea, Philippines, Samoa, Solomon Islands, Thailand and Vanuatu).

The objective of the meetings was to examine the risks and benefits of paying ransom to ransomware attackers by seeking answers to the following four key questions:

1. Should victims consider paying?
2. How can victims recover payment?
3. What cooperation is needed to facilitate recovery?
4. Can laws and regulations facilitate the recovery of ransom payments?

It is clear that in any attempt to provide a response to the threat of ransomware, it is necessary to consider the policies and measures that could be implemented to prevent such an attack from occurring. In a recent blog post, Chainalysis indicated that the revenue of ransomware actors had decreased significantly in 2022 owing to heightened awareness of security measures, showing that proactive policies and measures can be highly effective in preventing malicious actors from succeeding in their efforts.[1] Thus, rather than merely answering questions about possible responses to extortion, it is also important to consider and implement preventive measures that could protect the target in the first place.

Encapsulating the experiences shared by the Member States represented at the expert group meeting and the recommendations formulated over several days of discussions, the present paper attempts to bring to the reader's attention all possible issues that need to be considered in the decision-making process when preparing for or responding to a ransomware incident.

[1] Chainalysis, "Ransomware revenue down as more victims refuse to pay", 19 January 2023. Available at https://blog.chainalysis.com.

Chapters I to IV summarize the findings of the three meetings in the form of detailed recommendations designed to guide policy decisions regarding the questions set out above. Chapter V offers an outlook on a wider spectrum of policies that can guide the decision-making process at all stages of a ransomware attack and enable organizations to identify the most effective responses.

Overall, the paper underscores the significance of developing a comprehensive regulatory framework on virtual assets as a critical precondition for an effective response to the ransomware threat. It is crucial to establish policy guidelines that can aid organizations in preventing and responding to ransomware attacks efficiently. The lack of specialized capacities to monitor, detect and trace virtual asset transactions highlights the need for international cooperation among Governments, the private sector and academia to combat this growing threat globally. To address those gaps successfully, it is essential to foster information- and data-sharing on existing cases, innovative investigative techniques and effective solutions, as well as to implement comprehensive and sustainable capacity-building programmes tailored to the individual needs of Member States.

Lastly, enhancing the capabilities of Member States in the areas mentioned above will equip them to combat all types of criminal activity that involve virtual assets, both now and in the future. The establishment of effective government structures and a regulatory framework in this domain will contribute not only to the development of secure digital economies, but also to improving the well-being and financial security of societies. Such initiatives will help to build trust in digital economies and promote the safe and secure use of virtual assets, thereby contributing to the long-term prosperity of individuals and communities alike.

The present paper does not endorse or promote the payment of ransom and generally advises against it. However, it does explore potential scenarios in which payment has already been made or is being considered on the basis of "force majeure". The paper is not prescriptive, nor is it intended to impose any viewpoints on Member States. Instead, its purpose is to inform and guide policymakers in their approaches to managing ransomware incidents. It is ultimately up to each jurisdiction to determine the best course of action within the framework of its national system.

CHAPTER I.

Should victims consider paying?

Before addressing this question, it is important to define the term "victim" within the context of the present paper. A victim of a ransomware attack is an individual, organization or State entity whose information technology equipment, infrastructure or systems have been attacked and compromised by malicious software known as ransomware.

A quick Internet search will lead to the widely acknowledged advice for those affected by ransomware: "Do not pay the ransom."

While no States have issued any definitive rulings regarding ransomware payments, largely owing to the inherent complexity and unpredictability of each unique case, some Member States provide direct guidance not to pay.[2] In the United States of America, for example, the Joint Ransomware Task Force, which includes representatives from the Cybersecurity and Infrastructure Security Agency, the National Security Agency, the Federal Bureau of Investigation and the Multi-State Information Sharing and Analysis Center, does not recommend paying ransom and additionally warns that such payments may give rise to sanctions risks.[3] Others strongly discourage paying or do not condone making payments to cybercriminals.

In a nutshell, ransomware victims may consider paying the ransom to recover data to which they have lost access after a thorough analysis of the incident has demonstrated that:

- There is no possibility of recovering the data (i.e. no backups or only infected backups exist).
- No decryption tools for the particular strain of ransomware are known to exist.
- The cost and impact – financial or otherwise – of rebuilding the data from scratch prohibitively exceed the amount of ransom demanded, or the estimated further harm or damage is not acceptable.
- Most importantly, the ransomware actor has demonstrated the ability to decrypt the data by providing the decryption key (or keys) for a reasonably important sample of encrypted data.

[2] Joint Ransomware Task Force, "#StopRansomware guide", May 2023. Available at www.cisa.gov.

[3] United States Department of the Treasury, Office of Foreign Assets Control, memorandum of 21 September 2021 entitled "Updated advisory on potential sanctions risks for facilitating ransomware payments". Available at https://ofac.treasury.gov/.

Although the conditions listed above may seem reasonable and simple, there are various complex aspects that must be discussed and defined.

However, this is only the starting point for anyone facing this threat. The practical course of action to be chosen by a ransomware victim will depend on a multitude of factors and potential risks, which will be explored in greater detail in this chapter and the ones that follow.

RANSOMWARE AND VIRTUAL ASSETS

Ransomware perpetrators usually request payment in the form of virtual assets, as they provide a high level of confidentiality and are difficult to track. Although some ransomware strains accept or are suspected of accepting ransom payments in XRP (Ripple)[a] and Ether,[b] Bitcoin remains the most commonly utilized cryptocurrency for such attacks. Cryptocurrencies such as Bitcoin, Ether and XRP are pseudonymous, meaning that they do not provide information on the identity of the parties involved in the transaction. Monero, an anonymity-enhanced cryptocurrency that employs various technologies to conceal transactions and prevent user identification, has gained popularity among ransomware operators in recent years. Unlike Bitcoin and other alternative coins ("altcoins") that have public and transparent blockchains that enable transaction tracing, Monero transactions cannot be traced without obtaining additional cryptographic keys, making it difficult for blockchain investigators to identify the recipient of a payment.

[a] Pete Evans, "Hackers threaten to reveal personal data of 90,000 Canadians caught in bank hack", CBC News, 29 May 2018. Available at www.cbc.ca.

[b] L. Abrams, "HC7 planetary ransomware may be the first to accept Ethereum", Bleeping Computer, 9 January 2018. Available at www.bleepingcomputer.com.

Intangible risks of paying ransom

Some of the intangible hazards that should always be taken into account as compelling reasons against paying ransom, and that must be evaluated in each individual case, include:

- Incentivizing criminality, from illicit enrichment to funding transnational organized crime and terrorist financing
- Legality and compliance issues associated with making ransom payments
- Likelihood of recovering data and the possibility of continued extortion (double, triple, etc.)
- Reputational and/or political damage

In a context without regulation, the above-mentioned risks are very individual and subjective from the point of view of each victim. They may be outweighed by other factors, which are, in most cases, determined by circumstances such as the victim's primary line of business, the sensitivity of exfiltrated data, or the potential effects on the rights of others. An example of such an effect would be a case in which an organization responsible for maintaining critical infrastructure is targeted by ransomware, rendering that infrastructure inoperative and endangering people's lives as a result.

When payment is not possible

The idea of considering paying ransom in itself implies the availability of the funds demanded in exchange for the encrypted data. If no funds are available or can be made available to the victim, the discussion stops there, without further arguments. In the case of State victims, the legal authorization to move funds for such a purpose might be an additional challenge in a situation of force majeure that would require payment, such as cases involving certain risks of loss or severe effects on human lives. That would be an exceptional case in which even attempting to negotiate the amount of ransom is not a viable option. In such cases, victims should first opt to either seek assistance in recovering the encrypted data using available public resources, for example a national computer emergency response team (CERT) or computer security incident response team (CSIRT), the Forum of Incident Response and Security Teams (FIRST) network[4] or the No More Ransom project,[5] or attempt to recover and rebuild the data from scratch.

Explicit legal ban on paying ransom

Another serious consideration to take into account is the legality of paying ransom. While there may be several reasonable arguments in favour of paying ransom under certain circumstances, doing so may simply be impossible or constitute a direct violation of national law by those responsible for taking and/or executing such a decision, with all the legal consequences it may entail. In addition, paying ransom may also give rise to sanctions imposed by the relevant authorities owing to potential breaches of data protection regulations.

Countries with legislation that specifically prohibits paying ransom to extortionists could explore legal avenues that allow exceptions in certain cases if the victim can justifiably prove that paying the ransom is the only practical solution. An example of such a scenario would be when there is no way to recover or recreate vital data or when doing so would incur prohibitive costs or pose a serious risk to human lives, and when the ransomware attacker can demonstrate the ability to decrypt a sample of the data, thereby increasing the chances of recovery. While the present paper does not advocate paying ransom, in such a situation it is crucial that victims report ransomware incidents and work closely with national law enforcement agencies, their own legal advisers, relevant international organizations and other partners in the planning and execution of operations to trace and recover ransom payments.

[4] The FIRST network is a global non-profit association that brings together computer security incident response teams and security professionals from around the world. Its primary mission is to enable incident response teams to respond to security incidents more effectively and to prevent and mitigate cyberthreats (https://first.org).

[5] The No More Ransom project is an initiative of the National High Tech Crime Unit of the Netherlands Police, the European Cybercrime Centre, Kaspersky and McAfee with the goal of helping victims of ransomware attacks retrieve their encrypted data without having to pay the criminals (www.nomoreransom.org).

Proof of ability to decrypt and recover data

Even if the ransom is paid, there is no guarantee that the encrypted data will be decrypted effectively using the key provided by the ransomware operator. Therefore, in cases where the victim is considering paying ransom owing to the gravity of the assessed risk, when negotiating the ransom amount and conditions, it is advisable to ask the ransomware actor to demonstrate the ability to decrypt the data by providing the decryption keys for a sample of the files. Although it is typically assumed that all of the data are encrypted using the same algorithm, it is best to confirm the recoverability of the files that are most crucial for a speedy recovery.

Although the probability of receiving a decryption key or any tool to retrieve data from the ransomware attacker is a crucial factor in determining whether to pay the ransom, it may not be possible if the ransomware actor refuses to communicate or negotiate. Nonetheless, an attempt to start negotiations should be made.

Threat of continued extortion

The repeated use of extortion tactics, often known as double and triple extortion, has become increasingly prevalent since 2019. Attackers who use such tactics steal data by conducting network reconnaissance in the victim's system to determine the high-value assets and exfiltrate them to their own storage networks before encrypting the data. They then increase pressure on the victim to pay the ransom by threatening to sell or reveal the data online or to attack the victim's customers or partners. In such cases, victims are advised to assume that the sensitive data will eventually be released even if the ransom is paid and to take steps to minimize the damage.

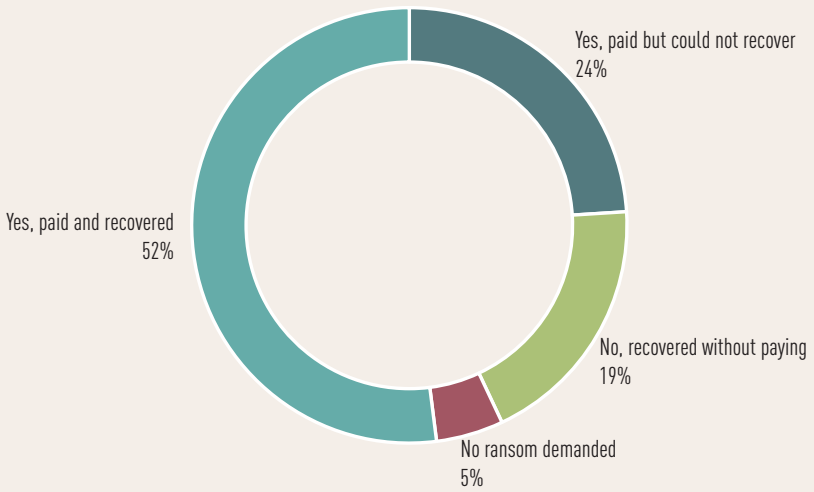
Overall, it is crucial for ransomware victims to address the cybersecurity vulnerabilities that permitted the initial attack, thereby avoiding repeated victimization due to the same weaknesses. Documented instances of double or triple extortion illustrate that, if such vulnerabilities persist, negotiating ransomware payments may cease to be a viable option.

Perceived advantages of paying ransom

Undoubtedly, there is nothing advantageous in parting with a large sum of money just to recover stolen data; in addition, the recovery itself is not an instantaneous process, and it costs time and money to ensure that the restored systems are clean and secure. This section explores some of the possible aspects of a ransomware incident that victims may perceive as advantageous in such a situation.

As paradoxical as it may sound, the traceability of commonly demanded cryptocurrencies means that making a ransom payment may actually aid law enforcement investigations and help in the recovery of funds.

FIGURE I. RESPONSES TO THE SURVEY QUESTION "WERE YOU ABLE TO RECOVER THE DATA AFTER PAYING RANSOM?"



According to a survey of 1,000 leaders in the information technology sector conducted by an independent research firm in 2022,[6] 52 per cent of respondents reported the successful recovery of their data after paying the ransom, while 24 per cent of those who paid the ransom were still unable to recover their data (see figure I). There is a somewhat reasonable chance of getting the encrypted data back, which is a positive development on its own, especially in high-profile cases of victims that operate critical infrastructure or when a business impact analysis confirms that it is less expensive to pay the ransom than to rebuild the data. While it is impossible to ensure complete or even partial data restoration, it is considerably more probable than not, as the primary driving force behind ransomware groups is financial gain. Not fulfilling their promises would have a detrimental impact on their illicit earnings. However, the statistics presented in the report cited above indicate that paying the ransom does not guarantee the recovery of data encrypted by ransomware.

Another frequently perceived advantage to paying ransom, based on the nature of the data that have been encrypted, is the potential reduction of the likelihood of the data being sold or distributed on the Internet. Victims may regard such a course of action as a means of avoiding violations of data security laws, controlling the disruption of their business and minimizing harm to their reputation. However, that perception is false and dangerous, since – as mentioned in the section on the threat of continued extortion – victims should assume that sensitive data have already been extracted and act as if the data will be sold or otherwise made public.

[6] Veeam Software, *2022 Ransomware Trends Report*. Available at https://go.veeam.com.

As mentioned above, if payments are made, it may be possible to investigate the crime by tracking cryptocurrency transactions in order to uncover the identity of the ransomware attackers and retrieve the funds. As this crime is often borderless in nature, it is crucial that victims report incidents to law enforcement authorities and that the competent authorities make use of all available means, including international law enforcement channels. Coordination with law enforcement authorities and private sector entities, such as virtual asset service providers (VASPs) and blockchain analytics companies, during the investigation of ransom payments can provide valuable investigative leads. Thoroughly examining the communications exchanged during ransom negotiations and after payment can also be important for investigators, as those communications can provide valuable information about the attackers and their methods.

Lastly, although paying ransom can have negative impacts on victims in terms of financial loss and reputational damage, it could provide the impetus for them to improve their internal security systems, policies and strategies. By discovering the strengths and weaknesses of its own network infrastructure, cybersecurity and resilience measures and incident response policies, as well as its capacity-building, training and awareness-raising policies for personnel, an organization can implement necessary changes at various levels in order to improve its defences against future ransomware attacks. Ransomware victims who did not pay ransom, whether out of compliance with legal requirements or owing to insufficient funds or an effective incident response plan that facilitated data recovery, can still learn from the experience.

CHAPTER II.

How can victims recover payment?

Managing ransomware incidents is often viewed as a weighing of costs and benefits between the attacker and the victim. For the attacker, the cost of carrying out the attack is relatively low, while the profits can be substantial. For victims, although paying the ransom can be expensive, many are prepared to incur the cost because of a perceived trade-off: they might believe that the repercussions of not paying could be more significant than the expense of paying. Victims who do pay, however, may unintentionally encourage more ransomware attacks in the future by demonstrating to ransomware attackers that their efforts are profitable. To minimize and prevent the occurrence of ransomware incidents, it is crucial for organizations to cultivate a security-conscious culture in order to defend against ransomware attacks, and to report ransomware incidents to law enforcement or other appropriate authorities in a timely manner.

To increase the chances of recovering ransom payments made in cryptocurrencies, it is important for victims to be proactive and prepared to respond quickly and efficiently. That includes investing in cybersecurity infrastructure and reporting to law enforcement authorities as soon as a ransomware incident occurs in order for them to identify relevant cryptocurrency addresses and freeze accounts at VASPs as necessary. Even if an organization is otherwise prepared for a ransomware attack, it is important to take these actions and measures as soon as possible in order to increase the chances of successful ransom recovery.

Incident reporting

Complying with legislation is crucial in the case of a ransomware attack. In some jurisdictions, it may be mandatory to inform law enforcement and other relevant authorities within a specific time frame.[7] In addition, if the victim has cyber insurance that covers ransomware incidents, the appropriate legal procedures must be followed. It is important that victims contact law enforcement authorities at the national level as soon as possible and inform the relevant CERT/CSIRT

[7] Requirements for reporting ransomware incidents or data breaches differ from one jurisdiction to another. Deadlines for reporting span from two hours to 60 days after the discovery of the incident, depending on the victim's line of business and the sensitivity of the data. The text of the requirements often includes expressions such as "as soon as possible", "as soon as feasible", or "as soon as practicable".

(if one has been established). Law enforcement agencies can begin investigations and obtain assistance from international partners, financial institutions, VASPs and blockchain analytics companies. It is also important that financial institutions file the required reports if they identify suspicious transactions that may be linked to ransom payments or related money-laundering.

Information-gathering

Collecting information about the ransomware attack and the attacker is a crucial part of managing the incident. This includes obtaining details about the virtual asset wallet address or addresses to which the payment is requested, as well as analysing network traffic prior to the attack. The law enforcement authority should thoroughly examine the communications between the victim, its systems and the attacker for any useful information that could aid in the investigation. Collecting as much information as possible from all available sources increases the likelihood of a favourable outcome for the victim. In addition to the actions undertaken by law enforcement agencies in response to criminal activity, CERTs/CSIRTs (if established) play their own crucial roles. These teams are responsible for collecting and analysing cybersecurity-related data and trends. Their task is to identify potential threats and vulnerabilities and then develop effective strategies and policies to counteract them.

Cases of force majeure affecting human lives

In cases of force majeure, where the anticipated losses and impacts from a ransomware attack exceed acceptable damage levels – often in situations that pose the risk of a negative impact on human lives – negotiating ransomware payments may become a viable option to prevent more significant losses.

In such cases, utilizing the services of a specialized cybersecurity firm with extensive expertise in ransom negotiations and recovery may prove to be beneficial even if in-house expertise is available. The experience of specialized negotiators can provide a significant advantage in lowering the ransom amount, minimizing the impact of the attack and gathering evidence that can aid in identifying the perpetrators.[8]

It is recommended that a pre-vetted specialized cybersecurity firm (or firms) be part of the ransomware mitigation plan. If no such arrangement exists, law enforcement authorities and international partners may be able to provide reliable referrals.

In cases where paying ransom is contemplated, it is advisable to pay it in a cryptocurrency that is based on a public and transparent blockchain so as to enable the tracing of all transacting addresses. Bitcoin, which is widely used for ransom payments, and alternative cryptocurrencies such as Ether, Litecoin and XRP all operate on public blockchains. However, Monero, an anonymity-enhanced cryptocurrency, is gaining popularity among ransomware actors as the

[8] Pepijn Hack and Zong-Yu Wu, "We wait, because we know you: inside the ransomware negotiation economics", posted by Aaron Haymore, NCC Group Research, 12 November 2021. Available at https://research.nccgroup.com.

currency in which they demand payment. Negotiating for payment to be made in Bitcoin or another traceable cryptocurrency is recommended, even if the attackers demand a lower amount in Monero or another anonymity-enhanced cryptocurrency. Criminals are aware of the traceability of certain cryptocurrencies and may increase the ransom amount to compensate for the cost of additional obfuscation of the funds.

Reporting ransomware incidents to law enforcement authorities can significantly improve the chances of recovering ransom payments, as it leads to better cooperation and coordination with VASPs at both the national and international levels. Such collaboration may give victims a strategic advantage over the attackers and allow for blocking and freezing of the funds when they are transferred to a centralized cryptocurrency exchange.

CHAPTER III.

What cooperation is needed to facilitate recovery?

Strong collaboration is needed among all stakeholders, including governments, private companies and citizens, for the successful recovery of ransom payments. Companies specializing in cybersecurity and blockchain analytics can offer their expertise to aid in investigating the movement of virtual assets and identifying the "off-ramps" utilized by criminals to convert their gains into cash. While law enforcement authorities and prosecutors investigate ransomware attacks and prosecute the perpetrators, financial institutions can play an important role in identifying and reporting suspicious activities that can be linked to cyberattacks such as ransomware incidents by detecting, reporting and blocking ransom payments. They may also be able to help victims recover their funds, often with the support of law enforcement authorities.

Awareness and education

To effectively combat ransomware crime, it is crucial to increase public awareness and education on several key aspects, including how ransomware criminals target and victimize organizations, the ways in which organizations can protect themselves against ransomware attacks, the importance of reporting attacks when they occur and the best practices to follow when responding to a ransomware attack. These efforts are beneficial not only for law enforcement, but also for society as a whole. Through education campaigns and public awareness initiatives, individuals can gain a deeper understanding of the crime and how to effectively respond to it.

Such campaigns and initiatives can be implemented through a variety of media, such as print advertisements, public service announcements and other forms of coverage. In addition, schools and community organizations can be encouraged to give informative talks on the topic. With adequate understanding, everyone can become more aware of the ransomware threat and how to detect it. This may lead to better reporting of the crime and more effective responses, ultimately contributing to reducing the prevalence of the crime.

National inter-agency cooperation

Inter-agency cooperation at the national level is vital to the successful recovery of ransom payments. Without collaboration among different government agencies, the complexities of this type of cybercrime can be difficult to disentangle and the necessary resources may not be available.

By working together, law enforcement and prosecution agencies, financial regulatory bodies, intelligence agencies and national CERTs/CSIRTs can share resources, such as specialist personnel, analysis, research and intelligence on the activities of criminal groups. Such collaboration can help to identify the source of the ransomware, the payment mechanism and the pattern of transaction flows. This is important for assisting victims in recovering their funds, as well as for identifying the perpetrators and providing evidence for prosecution. The agencies mentioned above should collaborate in streamlining the regulatory framework relating to the recovery of ransom payments.

One key aspect of national inter-agency cooperation is the involvement of law enforcement agencies, which can provide support in tracking down attackers and gathering evidence for prosecution. With their resources and expertise, law enforcement agencies can play a critical role in disrupting the activities of ransomware actors and preventing future attacks.

Another important aspect of national inter-agency cooperation is the ability to quickly identify related ransomware cases and possibly link the criminal actors behind them, as well as to find and assist victims of attacks. Such assistance could include providing victims with resources to help them recover their data and offering advice on how to prevent future attacks. It can also help to ensure that any payments made to the attackers are properly recovered and that recovered funds are used to support the victims of attacks.

In the case of ransomware attacks, CERTs/CSIRTs (if established) are generally well equipped to provide critical cybersecurity-related support to organizations that have been affected. Not only can they provide technical advice on how to mitigate the damage caused by the attack, but they can also assist in the recovery of encrypted data and, upon request, provide information to the law enforcement agencies investigating the incident.

Government agencies can develop regulations and policies to strengthen cybersecurity, bolster cybercrime prevention efforts and enhance resilience measures with a view to protecting against ransomware attacks and helping organizations recover from such incidents. For example, they can enforce stricter security standards and educate the public on best practices for avoiding ransomware attacks. Such inter-agency cooperation can lead to the development of more comprehensive and effective strategies for combating ransomware and ensure that organizations and individuals are better protected from this growing threat.

International cooperation

International cooperation between law enforcement agencies, financial regulatory bodies, asset recovery authorities and cybersecurity companies is considered essential for successful action to counter ransomware attacks. Cooperation among those entities not only aids in the technical aspects of data recovery, but also facilitates a comprehensive criminal justice response. It enables the global investigation of cybercrimes, supports the prosecution of offenders across jurisdictions

and fosters the sharing of crucial information and resources, thereby reinforcing global resilience against ransomware attacks. International organizations and regional asset recovery networks can provide the resources and expertise necessary to coordinate a response across multiple countries, thus allowing for more effective communication in forensic investigations, the collection of evidence and the coordination of the recovery process. Such cooperation can also help to ensure that all aspects of the response and recovery processes are properly addressed and that all parties involved are fully informed of the situation. Through collaboration, the expertise of countries with advanced capabilities in investigating ransomware threats and tracing virtual asset payments can be utilized to assist and build the capacity of States with less developed capabilities in this regard.

The prompt exchange of intelligence on ransomware attacks among CERTs/CSIRTs and the law enforcement agencies of Member States makes it possible to link related incidents, which, in turn, informs virtual asset-tracing efforts and advances investigations. In addition, such cooperation might help authorities to inform the public of the strategies employed by criminals and may enable individuals to take necessary precautions and avoid falling victim to such attacks.

Public-private collaboration/cooperation

Formal public-private partnerships provide a framework for collaboration and information-sharing between private sector organizations and government agencies. For example, financial institutions, such as banks and VASPs, can monitor transactions and identify ransom payments and, where appropriate regulation exists, are required to report to the competent authorities any suspicious activity potentially related to ransomware, while insurance companies may provide financial support for the recovery of ransom payments. Cybersecurity companies and incident response companies can provide technical information about the methods used by ransomware attackers, help to identify the sources of attacks and inform law enforcement agencies.

Informal public-private partnerships, such as information-sharing agreements, also play a critical role in the recovery of ransom payments. Financial institutions, insurance companies and cybersecurity companies can provide valuable information to law enforcement agencies, even in the absence of official partnerships. For example, cybersecurity companies can share information about the methods used by ransomware attackers, while insurance companies can provide proven guidance on the most effective recovery strategies.

By combining the resources of the financial sector, insurance companies and cybersecurity firms, it is possible to create a more comprehensive system that can better address the unique challenges posed by ransomware. Such partnerships also enable law enforcement agencies to access valuable information and intelligence in order to investigate and prosecute offenders.

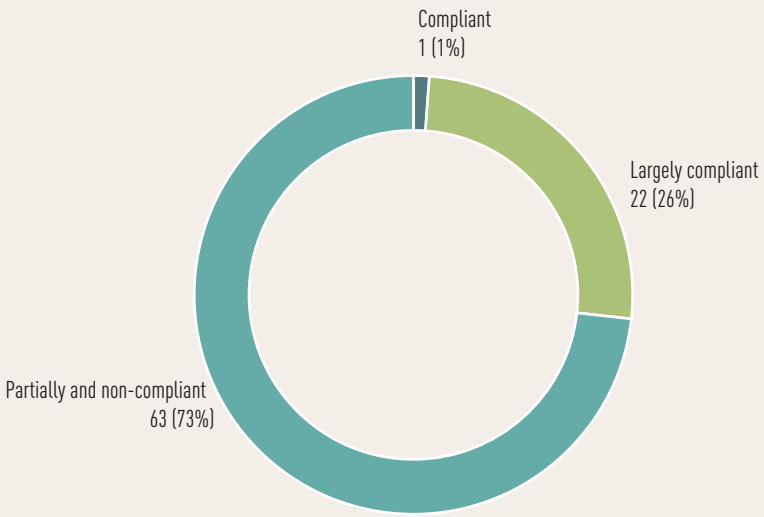
CHAPTER IV.

Can laws and regulations facilitate the recovery of ransom payments?

Currently, there is a legal void around ransomware payments. In this context, States can establish or amend the relevant legal and regulatory frameworks to effectively address the issue of ransom payments by implementing the international anti-money-laundering (AML) and countering the financing of terrorism (CFT) standards for virtual assets and VASPs, and by holding cyber-criminals accountable for their actions.

Advantages of regimes for countering money-laundering and the financing of terrorism in relation to virtual assets

FIGURE II. NUMBER (AND PERCENTAGE) OF JURISDICTIONS ASSESSED AGAINST REVISED METHODOLOGY ON RECOMMENDATION 15



The implementation of the international AML/CFT standards for virtual assets and VASPs can mitigate the degree to which ransomware criminals are able to use virtual assets and VASPs for the purpose of laundering their illicit proceeds. According to the Financial Action Task Force (FATF) report entitled *Countering Ransomware Financing*, "as of January 2023, of 86 jurisdictions that have been assessed against the revised Standards (Recommendation 15), 63 (73%) are partly or non-compliant with these requirements. Only one of the 86 jurisdictions have been assessed as fully compliant" (see figure II).[9] The FATF recommendations apply to virtual assets and VASPs, advocating a risk-based approach to virtual asset activities or operations and VASPs; supervision or monitoring of VASPs for AML/CFT purposes; licensing or registration; preventive measures, such as customer due diligence, record-keeping and reporting suspicious transactions; sanctions and other enforcement measures; and international cooperation. Implementing those measures can support the identification and disruption of ransomware-related money-laundering through the reporting by financial institutions of suspicious transactions that may be related to ransomware, through the collection of information by financial institutions that can inform law enforcement investigations, and through the existence of coordination mechanisms between national and international authorities, to name but a few examples.

Effective regulations for critical infrastructure

States are advised to introduce regulations that provide a framework for informed decisions regarding ransom payments and prevent them from becoming a revenue stream for cybercriminals. With regard to ransomware in particular, regulations governing measures for entities that operate critical infrastructure are of utmost importance, as a ransomware attack on such entities can have far-reaching consequences for the functioning of society.

When establishing regulations related to critical infrastructure, States must carefully evaluate the optimal degree of control, which may range from operational rules to administrative instructions. States also need to judiciously choose the most suitable legal field – be it administrative, civil or criminal law – to govern those rules.

Above all, it is imperative to ensure that such regulations are unambiguous and enforceable and that they include a mandatory requirement for reporting to the pertinent regulatory bodies and law enforcement agencies. This will ensure not only compliance but also the security and resilience of the State's critical infrastructure. The most crucial element, however, is to have proper measures in place to prevent future attacks and reduce the risk of ransom payments being used for illegal activities. It is vital to implement comprehensive cybersecurity measures, which should include conducting regular security audits, keeping software updated, enforcing strong password policies and providing employee training. All of those steps are essential in responding to cyberthreats.

[9] Financial Action Task Force (FATF), *Countering Ransomware Financing* (Paris, 2023), para. 33.

Minimizing the risk of supporting illegal activities

Attackers may attempt to exploit weaknesses in regulatory and legal frameworks relating to cybersecurity and data protection in order to conduct attacks with minimal risk of being caught or punished. Ransomware-related regulation should be designed in a way that encourages organizations to develop comprehensive plans and establish relevant management systems in accordance with International Organization for Standardization (ISO) standards, while avoiding the creation of explicit provisions that attackers could take advantage of. Such plans and systems may include an information security management system and an incident management plan,[10] a business continuity plan and a disaster recovery plan,[11] and a privacy information management system.[12] In addition, regulations should include special provisions for cases that could be regarded as terrorism financing in order to ensure that organizations are not inadvertently supporting illegal activities. Those provisions should be carefully crafted to ensure that organizations are given the necessary guidance and support to respond to ransomware attacks that exhibit such elements.

[10] International Organization for Standardization, ISO/IEC 27001:2022 (October 2022).

[11] ISO 22301:2019 (October 2019).

[12] ISO/IEC 27701:2019 (August 2019).

CHAPTER V.

Ransomware incident decision-making

While chapters I to IV are primarily focused on issues related to responses with regard to ransom payments, this chapter takes a more comprehensive approach to dealing with a ransomware incident and provides an overview of all the aspects involved in decision-making in relation to a ransomware attack, from prevention policies to investigation and post-incident analysis. The decision tree shown in figure III illustrates the main stages of this process, which will be described in greater detail in the sections that follow.

Prevention

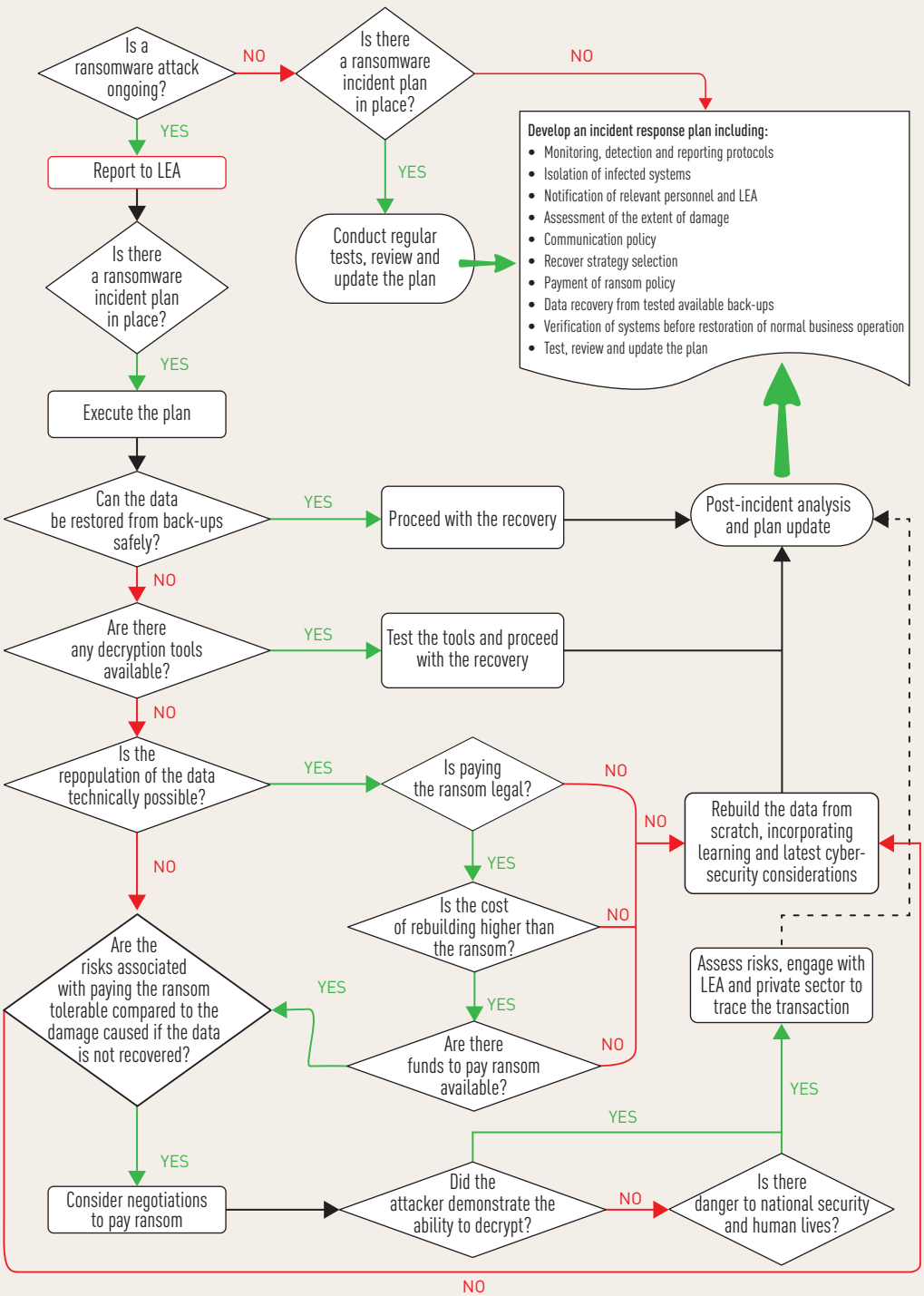
Ransomware prevention policies cover the questions to be asked in order to determine the appropriate course of action to be taken in the event of a ransomware attack. If an organization successfully implements these policies, the chances of recovering lost data without paying ransom to the attackers can be very high. The policies relate primarily to topics already mentioned in the present paper, such as data backups, cybersecurity strategies and policies, education and training on cybercrime – with particular emphasis on ransomware – and cyber insurance, if appropriate.

Education and awareness-raising

Education and awareness-raising policies play a crucial role in preventing ransomware attacks at the organizational level. To that end, organizations may consider implementing the following:

- Security awareness training. Provide security awareness training to all employees, including information on how to identify and avoid phishing scams and spear-phishing attacks that specifically target the organization, and best practices for secure data management.
- Incident response training. Conduct regular incident response training to ensure that employees are prepared to respond effectively to a ransomware attack, know what actions to take, and have a clear understanding of their respective roles and responsibilities.
- Regular security and information updates. Provide regular security updates and patches to all employees and keep them informed about the latest threats and vulnerabilities.
- Access control training. Train employees on access control policies and how to use them to prevent unauthorized access to sensitive data and systems.

FIGURE III. DECISION-MAKING PROCESS IN RESPONSE TO A RANSOMWARE ATTACK



Abbreviations: LEA, law enforcement authority.

- Bring-your-own-device training. Provide training on bring-your-own-device policies and guidelines to ensure that employees know how to access the organization's data and systems securely using their personal devices.
- Encryption training. Train employees in the use of encryption tools and how to use them to protect sensitive data from unauthorized access or theft.
- Third-party security training. Provide training to employees on third-party security policies and guidelines and on how to ensure that third-party vendors and service providers are following proper security protocols.
- Incident reporting training. Train employees on how to report security incidents, including suspected ransomware attacks, to the appropriate personnel or the information technology department, and provide clear reporting channels and procedures for such incidents.

Backup and recovery

A comprehensive data backup and recovery policy is crucial to withstanding a ransomware attack. Although the backup and recovery strategy is typically included in the general cybersecurity strategy, the present paper emphasizes its paramount importance in protecting against a ransomware attack. Some considerations to include in the policy are as follows:

- Backups. Develop a backup strategy that includes regular and automated backups of critical data to secure online, offline or offsite locations.
- Testing. Test backup systems and procedures regularly to ensure that they are functioning as intended and normal operations can be restored quickly in the event of an attack.
- Retention. Develop a retention policy that defines how long data will be kept and how frequently it will be backed up.
- Access control. Control access to backup systems and data to prevent unauthorized access or tampering.
- Incident response plan backups. Include specific procedures for responding to a ransomware attack and restoring data from backups in the organization's ransomware incident response plan.

Risk assessment

In managing a ransomware incident, the organization's level of preparedness and the perceived severity of the attack are the two key factors. The severity of the attack is determined by the types of systems affected, the data encrypted, the relative risk to national security interests and data privacy concerns. The severity can generally be categorized as high, medium or low. On the other hand, preparedness for a ransomware attack can simply be categorized as high, where an incident response plan and trained staff are available, or low, where they are not. Although intermediate preparedness levels might exist, the organization in question should be able to identify its own level of preparedness in each situation. The extent of preparedness is primarily dependent on the organization's internal capacities and understanding of the importance of securing its critical data for business continuity. Organizations that value their data assets as

critical to their operations usually implement incident response plans and provide training to their staff to support those plans.

The table below outlines a typical course of action for each combination of attack severity and preparedness level.

ATTACK SEVERITY VERSUS PREPAREDNESS LEVEL DECISION MATRIX

ATTACK SEVERITY \ PREPAREDNESS LEVEL	HIGH Incident response plan in place, staff are trained	LOW No incident response plan and staff are not trained
HIGH Critical infrastructure, public safety, national security systems	Follow the incident response plan and engage external experts as necessary	Seek external assistance and follow incident response best practices
MEDIUM Business-critical systems, risk of data loss	Follow the incident response plan and consider engaging external experts as necessary	Seek external assistance and follow incident response best practices
LOW No immediate risk to critical operations or data loss	Follow the incident response plan and conduct a thorough investigation to identify the root cause of the attack	Seek external assistance and follow incident response best practices

Incident reporting and documentation

Reporting a ransomware incident is critical in managing its aftermath and mitigating potential harm. It is vital to have a clear plan in place to report such an incident to the appropriate internal and external stakeholders, and to follow specific guidelines for communication and documentation. Those measures can help to protect the organization from further damage, minimize disruptions to its operations and increase the chances of a successful post-incident analysis.

The criteria for reporting and notifying stakeholders in a ransomware incident depend on the severity of the attack, the type of data involved and the internal policies of the organization. In most cases, incidents that affect sensitive or classified data or that impact national security and critical infrastructure should be reported to the relevant authorities immediately. Other critical factors that may require notification include any legal obligations, contractual obligations or specific industry regulations.

Internal communication guidelines must also be in place to ensure that all relevant personnel are informed of the situation and are aware of their roles and responsibilities. Such personnel should include senior management, staff in information technology, legal and human resources departments, and any other relevant parties. The communication must be timely, accurate and consistent, and it must include updates on the status of the incident and the steps being taken to manage it. It is also essential to maintain clear communication channels and to ensure that all parties understand the confidentiality requirements of the situation.

External communication guidelines should be in place for notifying external stakeholders, such as customers, suppliers and partners. Organizations should notify stakeholders in a clear and transparent manner and provide accurate and up-to-date information on the incident and the steps being taken to address it. The communication should be targeted and appropriate to the audience and may involve multiple channels, including email, social media and press releases.

Documenting all processes and procedures is essential for a successful post-incident analysis. The documentation should include all relevant information, such as the timeline of events, steps taken to address the incident and communication logs. It should be thorough, accurate and stored in a secure location for future reference.

Cybersecurity

Given the widespread prevalence of ransomware, implementing an organization-wide cybersecurity strategy is of utmost importance. Regardless of the sensitivity or value of their data, organizations of all sizes should implement an appropriate set of policies to safeguard their interests. While organizations that are critical to the normal functioning of society must be legally required to implement such measures, other types of organizations may choose to do so on the basis of their business objectives and market considerations.

Cybersecurity policies that organizations can adopt to help prevent ransomware attacks include the following:[13]

- Incident response. Develop an incident response policy that outlines the steps to be taken in the event of a ransomware attack. This policy should specify the roles and responsibilities of each member of the incident response team and include communication procedures, escalation paths and procedures for notifying law enforcement, clients and vendors.
- Regular updates. Implement a regular update policy to ensure that all software and hardware, including operating systems, applications and security software, are kept up to date and patched against known vulnerabilities.
- Network segmentation. Segment the corporate network to reduce the impact of an attack and ensure that backup data are not compromised. This policy should specify how data flow through the network, who has access to each segment and how data are transmitted between segments.
- Access control. Implement an access control policy that restricts access to sensitive data and systems to authorized users only, and accord them the minimum privileges necessary to perform their respective jobs.
- Acceptable use. Establish an acceptable use policy with guidelines for the acceptable use of the organization's systems, devices and networks. The policy should include best practices for avoiding ransomware attacks, such as not clicking on suspicious links and not downloading unknown attachments.

[13] The policies listed here can be implemented as part of the organization's implementation of ISO/IEC 27001:2022 of October 2022.

- Monitoring. Establish a monitoring policy that specifies the tools and techniques used to monitor systems for signs of potential ransomware attacks, such as unusual network activity and unauthorized access attempts.
- Remote access. Develop a remote access policy with guidelines for accessing the organization's systems and data from remote locations, including the use of virtual private networks and other secure access protocols.
- Third-party security. Establish a third-party security policy that outlines the security requirements for third-party vendors and service providers. The policy should specify the procedures for conducting due diligence reviews and monitoring the security practices of third parties that have access to the organization's systems and data.
- External assistance. Establish relationships with external experts, such as incident response teams, legal counsel and law enforcement, to provide additional support in the event of an attack.

Cybersecurity insurance

As part of broader cybersecurity insurance policies, ransomware insurance is becoming more widespread as businesses become more aware of the risks associated with ransomware attacks. Such insurance may prove to be extremely worthwhile in a ransomware incident because it can provide financial protection to an organization in the event of a ransomware attack and cover the costs of ransom payments, data recovery and other related expenses. In addition, such insurance often covers access to incident response services, which can minimize the impact of an attack, and offers risk assessment support, thereby helping to identify potential vulnerabilities in the organization's cybersecurity strategies and enabling it to take steps to reduce the risk of future attacks.

At the same time, it is prudent to exercise caution regarding cybersecurity insurance policies for ransomware attacks. There is a potential risk that such policies could inadvertently hinder criminal investigations and the reporting of ransomware incidents. Cybersecurity insurance policies may facilitate quick settlements of ransom demands, which may circumvent the imperative of engaging law enforcement immediately, potentially perpetuating the cycle of ransomware criminal activity. This situation underscores the uncertainties and complexities associated with ransomware incidents and their potential implications for law enforcement and cybersecurity.

Cybersecurity insurance coverage that can be useful in the event of a ransomware attack includes the following:

- Ransomware protection. Insurance policies can provide coverage for costs associated with a ransomware attack, such as ransom payments, legal fees and data recovery expenses.
- Incident response services. Many insurance policies cover access to incident response services, which can provide immediate support and guidance in the event of a ransomware attack.
- Cybersecurity risk assessment. Insurance providers may offer risk assessment services to help organizations identify vulnerabilities in their cybersecurity strategies and provide guidance on how to mitigate those risks.

- Business interruption. Insurance policies may include business interruption coverage to protect organizations against lost revenue and other expenses resulting from a ransomware attack.
- Public relations. Insurance providers may offer public relations coverage to help an organization manage its reputation following a ransomware attack.
- Data breach liability. Insurance policies may include data breach liability coverage to protect organizations against claims arising from the exposure of personal or sensitive data.
- Cyberextortion. Insurance providers may offer coverage for extortion attempts, including those that involve the threat of a ransomware attack.
- Social engineering fraud. Insurance policies may provide coverage for losses resulting from social engineering fraud, such as phishing scams or other forms of social engineering attacks, which are known to be among the main vectors of ransomware infection.
- Forensic investigations. Insurance policies may provide coverage for forensic investigations, which can help organizations to determine the cause and extent of a ransomware attack.
- Data recovery. Insurance policies may include data recovery coverage, which provides financial support for the cost of recovering lost or corrupted data following a ransomware attack.

It is worth noting that, at the time of writing, cybersecurity insurance was not universally available in all Member States.

Incident management

When a ransomware incident occurs, the organization should implement several plans and policies to effectively respond to the incident and minimize its impact, starting with the incident response policy and proceeding with the business continuity and disaster recovery plans. The initial step after discovering the incident is to evaluate the impact and risks involved. Depending on the organization's profile, a task force consisting of internal and, optionally, external stakeholders may need to be formed to support the decision-making process. The task force should employ the knowledge and expertise of all its members to determine the extent of the infection, establish containment measures and suggest eradication approaches. Relevant digital evidence should be gathered at the outset of the incident to aid in the assessment and future investigation to be conducted internally and/or by law enforcement agencies. International partners should be contacted, either through existing channels or intergovernmental agencies, to obtain the most recent knowledge and experience related to a specific strain of ransomware. It is also beneficial to ascertain whether decryption tools are available for the specific type of ransomware.[14]

[14] See, for example, No More Ransom (www.nomoreransom.org) and the websites of other cybersecurity companies.

Investigation preparedness

Having in-house capabilities to investigate ransomware incidents and other cyberattacks can play a key role in rapidly identifying the origin and scope of a ransomware attack. Moreover, it can yield valuable intelligence that can be leveraged during ransom negotiations if that route is deemed necessary. While not all businesses and organizations may be willing or able to establish comprehensive internal investigative capacity, it is a vital asset for those enterprises that operate critical infrastructure and handle significant volumes of sensitive data.

Organizations should consider establishing points of contact in local law enforcement agencies and CERTs/CSIRTs. Those points of contact can provide valuable assistance in identifying and tracking the actors behind ransomware attacks. They can also provide critical insights into the latest ransomware variants and trends.

Tracing transactions and recovering ransom payments

Tracing ransomware transactions to the perpetrators and recovering ransom payments require a wide range of technical, legal and financial capacities. They are complex and challenging tasks that require a high level of expertise, national and international inter-agency collaboration and access to advanced technology.

The pervasive, borderless nature of the ransomware threat should encourage Member States to develop and maintain capabilities to investigate virtual asset-facilitated financial crime in line with the international AML/CFT standards, from the detection of illicit transactions to the seizure and forfeiture of virtual assets. Many countries have not yet implemented the international AML/CFT standards relating to virtual assets and VASPs. FATF is developing measures to support countries with less developed capabilities that are seeking to make progress in the implementation of those standards and has published updated guidance for a risk-based approach to virtual assets and VASPs,[15] which outlines how the AML/CFT standards apply to them.

Capabilities for tracing and recovering virtual assets

Member States may consider developing some of the most critical policies and capabilities to be able to trace and recover virtual assets, including:

- Developing a comprehensive legislative framework that includes the following provisions:
  - A requirement to report ransomware incidents and related payments to law enforcement agencies and/or financial regulators within the shortest possible time frame (preferably within 24 hours, but no more than 72 hours, of becoming aware of the occurrence)[16]
  - A requirement for VASPs to keep records of all transactions relating to ransom payments, as they can help the authorities to trace and recover virtual assets

[15] FATF, *Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers* (Paris, 2021). Available at www.fatf-gafi.org.

[16] Prompt notification of ransomware incidents and/or payments should be made to the appropriate authorities as quickly as possible, including the basic information available at the time of the notification. A subsequent obligation to provide more comprehensive details at a later stage should also be part of the reporting process.

  - A requirement to implement the "know your customer" principle and anti-money-laundering policies and procedures, and to cooperate with the relevant authorities in the investigation of ransom payments, in line with the FATF guidance for a risk-based approach to virtual assets and VASPs[17]
  - Penalties for VASPs that do not comply with these requirements
- Developing the capacity to identify, trace and de-obfuscate virtual asset transactions and identify their recipients, by providing training as part of the national professional development system. This will help to ensure that the following relevant agencies and actors possess the necessary knowledge and skills and can sustain them over time:
  - Financial intelligence units
  - Law enforcement agencies
  - Prosecutors and the judiciary
  - Financial regulators (supervisory and monitoring authorities)
  - Asset management authorities
- Developing and periodically reviewing, in coordination with relevant international organizations:
  - Standard operational procedures on the detection, confiscation and management of virtual assets
  - Operational guidelines on the investigation and prosecution of crimes facilitated by the use of virtual assets
  - Templates for information requests to foreign VASPs, mutual legal assistance requests, suspicious transaction reports, seizure orders and court decisions, among others.

[17] See FATF, *Updated Guidance*.

Conclusion

In just over a decade since its introduction, a novel asset class has swiftly established itself outside the traditional financial system. This phenomenon is largely attributed to the development and widespread adoption of the Internet as a mass medium and to the advancement of cryptography as a scientific field. The outcome of those developments, referred to in the present paper as "virtual assets", but more precisely categorized as "cryptoassets", represents a new financial instrument that is based on a decentralized, immutable ledger of anonymous transactions (blockchains) that are secured by a set of open cryptographic algorithms. The nature of cryptoassets is such that it is impossible to shut them down without significantly impeding or completely disrupting the existing functionality of the Internet.

Although the legal status of cryptoassets is still a matter of debate, the relationship between ransomware and those assets is bidirectional and complex. On one hand, the rise of cryptoassets has given ransomware operators a convenient, anonymous and difficult-to-trace method of receiving payments. This has likely contributed to the increase in ransomware attacks, as it reduces the risk for attackers and makes it easier for them to monetize their activities. On the other hand, it is also likely that the increase in ransomware attacks has driven up the use of cryptoassets for criminal purposes. As more attackers turn to ransomware as a method of generating income, the demand for anonymous, untraceable payment methods has increased. So, while it is arguable whether the rise of cryptoassets has facilitated the increase in ransomware or the increase in ransomware has increased the use of cryptoassets for criminal purposes, the absence of central authorities behind cryptoassets, as well as the difficulty of attributing transactions, has certainly caused a significant paradigm shift that has caught financial regulators and law enforcement agencies off guard. Nevertheless, some progress has been made in developing techniques and regulations to tackle the risks relating to these assets.

The decision whether to pay ransom to recover data encrypted by ransomware is a complex one and requires careful consideration and evaluation of the risks, including the potential for further exploitation by criminals, the lack of a guarantee that the data will be fully recovered, the potential legal and ethical implications, and the chance that payment could encourage further criminal activity. While paying ransom may be perceived as the most practical solution in some situations, it should never be the first option considered by victims. In any event, reporting to law enforcement authorities should be considered mandatory. The recommended course of action is

either to utilize available public resources or to attempt to recover and reconstruct the data from scratch. In addition, the legality and compliance issues associated with paying ransom should be considered, not to mention the potential for incentivizing criminality, incurring reputational and political damage and inviting continued extortion.

If, however, after careful consideration and evaluation of the risks and the applicable legal frameworks, paying the ransom is deemed the only feasible solution, it is advisable to request proof of the ransomware perpetrators' ability to decrypt the data before beginning to negotiate the recovery of the data. In all cases, victims should consider engaging experienced professionals and informing law enforcement of the chosen course of action.

Reporting ransomware incidents to the law enforcement authorities within a prescribed time frame can significantly improve the chances of recovering ransom payments, as it may enable better cooperation and coordination with VASPs at the national and international levels. That, in turn, can give organizations a strategic advantage over attackers and allow for blocking and freezing of the funds when they are transferred to a centralized cryptocurrency exchange.

Gathering extensive information about the ransomware attack and the attacker is crucial to supporting the pursuit of justice. The identification of those responsible and the implementation of sanctions against such criminal activity are vital steps in reducing the current levels of impunity surrounding cyberattacks. The pursuit of justice, coupled with an organized response that includes financial investigations of virtual asset transactions and digital evidence-gathering, may have a positive impact on the likelihood of successfully recovering the ransom.

Effectively combating ransomware and, where applicable, recovering ransom payments require strong collaboration across all sectors, including government, private companies and citizens. Public awareness and education campaigns are necessary in order to increase knowledge about how ransomware criminals target and victimize organizations, and how organizations can protect themselves against ransomware attacks. National inter-agency cooperation is vital to the successful recovery of ransom payments, as it enables the sharing of resources, such as specialist personnel and intelligence on the activities of criminal groups.

For successful criminal justice action and data recovery in the event of a ransomware attack, international law enforcement cooperation is crucial because such attacks can originate from anywhere in the world and target individuals and organizations globally. Such cooperation requires the sharing of intelligence, resources and expertise to identify and mitigate the impact of the attack. Public-private partnerships also play a critical role in the recovery of ransom payments, as they combine the strengths of each sector and enable law enforcement agencies to access valuable information and intelligence to investigate and prosecute offenders.

The adoption of the international AML/CFT standards on virtual assets and VASPs is central to mitigating the risks of money-laundering related to ransomware. However, as mentioned in a recent FATF targeted update,[18] the majority of countries assessed to date have not achieved "largely compliant" status in the implementation of FATF recommendation 15, on new technologies. It is therefore critical that Governments prioritize compliance with those standards in order to effectively tackle the ransomware threat and ensure that cybercriminals are held

[18] FATF, *Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers* (Paris, 2022). Available at www.fatf-gafi.org.

accountable for their actions. The regulatory framework for ransomware must be designed to be adaptable to the constantly evolving nature of ransomware attacks and should consider advances in cybersecurity and data protection. Overall, the implementation of the recommended regulations can provide a comprehensive framework for organizations to make informed decisions on ransom payments and can prevent them from becoming a source of income for cybercriminals.

Organizations must have a comprehensive strategy in place to prevent, manage and recover from ransomware attacks. This involves the implementation of an incident response plan that includes backup and recovery policies, cybersecurity policies, continuous training of personnel, and education and awareness-raising initiatives. In the event of a ransomware incident, the organization must evaluate the impact and risks, form a task force and use a risk assessment matrix and a decision-making flow chart to determine the appropriate course of action. It is also crucial to report the incident to the appropriate internal and external stakeholders and maintain clear communication channels, while documenting all processes and procedures for future reference.

Mandatory reporting of ransomware incidents to law enforcement and regulatory authorities within a prescribed time frame and the implementation of policies in line with the international AML/CFT standards for the purpose of tracing and recovering virtual assets are crucial to combating ransomware. This requires the development of comprehensive legislative frameworks, strong and sustainable capacity-building efforts and the creation of harmonized operational guidelines in coordination with international organizations.

The United Nations Office on Drugs and Crime Global Programme against Money-Laundering, Proceeds of Crime and the Financing of Terrorism (GPML) and the Global Programme on Cybercrime are committed to enhancing their technical assistance and training programmes on virtual assets. One key objective of GPML is to assist the competent authorities of Member States in mitigating the risks of money-laundering and terrorist financing linked to the use of virtual assets. The programme encompasses various areas, including legislative, regulatory and supervisory support, national risk assessments, customized training and investigative guidance. Its ultimate goal is to assist countries in their compliance with FATF standards and enhance the effectiveness of their AML/CFT frameworks.

UNODC
United Nations Office on Drugs and Crime

Vienna International Centre, P.O. Box 500, 1400 Vienna, Austria
Tel.: (+43-1) 26060-0, Fax: (+43-1) 26060-5866, www.unodc.org

2306141