Singapore's Counter Ransomware Task Force Report

COUNTER-RANSOMWARE TASK FORCE REPORT
November 2022

Table of Contents

Foreword by the Minister-in-charge of Cybersecurity

Ransomware is a significant cyber threat we face today. Businesses in Singapore and around the world report that ransomware is one of their topmost cybersecurity concerns. In addition to being increasingly common, ransomware can have severe consequences as digital systems are now relied upon to support our economy and way of life. Recent attacks have sparked crises that have spilled over into the physical world, halting supply chains and disrupting essential services.

2. The criminal industry for ransomware is burgeoning because it is lucrative. With criminal groups offering Ransomware-as-a-Service, even unsophisticated criminals can have access to expanded capabilities to carry out their malicious activities. Fuelled by illicit monetary gains, an entire self-sustaining ecosystem has emerged, offering criminal services from access to targeted networks to money laundering services.

3. Although it is most often characterised as a cyber-attack, the solution lies not just in better cybersecurity, but also stronger cross-border law enforcement, and better measures against illicit finance and money laundering, especially where crypto assets are concerned.

4. This is why the Counter-Ransomware Task Force is an important platform. As a Government, we must be coordinated across the cybersecurity, law enforcement and financial regulation domains in order to address the ransomware problem effectively. Such coordination will also put us in better stead to work with other countries and jurisdictions to interdict illicit funds arising from ransomware attacks, trace the criminal actors responsible, and raise financial standards against the laundering of ransom payments, thereby putting a stop to this global industry. Cooperation across countries will

also help disrupt the ransomware business model, starve the ransomware criminal industry of profits, and eliminate safe havens for them.

5. This report should therefore be considered a blueprint for Singapore to counter ransomware effectively. I thank all the agencies and officers involved for their positive contributions towards a safe and secure cyberspace for our people and businesses.

Josephine Teo
Minister-in-charge of Cybersecurity,
Minister for Communications and Information and
Second Minister for Home Affairs

Executive Summary

The ransomware threat has grown significantly in scale and impact and has become an urgent problem for all digitally connected countries, including Singapore. It is also inherently an international problem, as attacks are conducted from across borders, and jurisdictional lines are leveraged to launder money and evade justice.

The Counter-Ransomware Task Force (CRTF) was commissioned to convene Government agencies across relevant domains, capabilities, and operational plans to strengthen Singapore's counter-ransomware efforts and put Singapore in a better position to push for international action against the global ransomware threat. Both domestic and international efforts are mutually reinforcing, and one cannot be effective without the other. The CRTF comprises senior representatives from the Cyber Security Agency, Government Technology Agency, Infocomm Media Development Authority, Ministry of Communications and Information, Ministry of Defence, Ministry of Home Affairs, Monetary Authority of Singapore and Singapore Police Force, as well as support from the Attorney-General's Chambers.

The CRTF's findings and recommendations are intended as a blueprint to guide the Government and respective agencies' efforts to secure Singapore from ransomware attacks.

Between January and September 2022, the CRTF met six times and achieved several outcomes. First, it developed a consolidated model of the ransomware kill chain to facilitate a common understanding among agencies of the stages of a ransomware attack, as well as the required actions to prevent and mitigate the attack at each stage. Second, the CRTF reviewed Singapore's national position on ransom payments to ransomware attackers to determine if the current advice remained relevant amidst the growing ransomware threat. Third, the CRTF has recommended the policies, operational plans and capabilities the Government should consider, to contribute to international efforts to stem the global ransomware problem, and to secure Singapore from ransomware attacks. These recommendations will be taken up by the relevant Government agencies for further study and implementation.

The Growing Ransomware Threat

The problem of ransomware is urgent, even existential, for all digitally connected countries, including Singapore. Recent attacks[1] have shown that ransomware attacks have the potential to become serious threats to a nation's national security, economic security, and critical information infrastructure. While ransomware attacks in the past have tended to be isolated and sporadic, typically affecting individuals or a handful of computers in companies, there has clearly been a step-change in the scale and impact of ransomware attacks over the past years.

a. Scale. The ransomware criminal industry has evolved significantly and ransomware attackers are now able to launch attacks that target or lock up hundreds, if not thousands, of computers simultaneously. Many attacks increasingly work by exploiting software that is widely used in the supply chain, so that they can affect as many victims as possible.

b. Impact. Attackers have raised their ambitions, and are starting to target large companies, essential supplies and services, even governments, in hope of eliciting a larger ransom. This also means the impact of ransomware attacks has gotten more severe and can often spill over to cause physical world harms, such as the disruption of essential supplies of services and amenities, as well as government services. These developments indicate that ransomware must no longer be regarded only as a sporadic nuisance, but a potential national security threat that could disrupt our Critical Information Infrastructure (CII) or lead to the encryption or theft of government or otherwise sensitive data.

2. **Ransomware is inherently an international problem**. In a borderless cyberspace, cybercriminals can target their victims from afar. They take advantage of jurisdictional lines to move and launder illicit profits and evade law enforcement. Of the 137 ransomware cases reported by Singapore companies to SingCERT in 2021, most, if not all, the attacks originated from overseas.

3. **Ransomware is a criminal enterprise, fuelled by illicit gains**. The Ransomware-as-a-Service (RaaS) model places ransomware capabilities in the hands of

[1] In May 2021, a ransomware attack on the Colonial Pipeline Company caused the largest fuel pipeline in the East Coast of the United States of America to shut down operations for close to a week, affecting the supply of fuel to around 50 million customers. In that same year, meat giant JBS was also ransomed for the equivalent of US$11M after a major cyber-attack that affected its facilities in the US, Canada and Australia, resulting in food supply chain disruptions and price surges. This year, nearly 30 Costa Rican government and public institutions were hit by ransomware attacks, including the Ministry of Finance, leading to the government declaring a state of emergency.

anyone who has intent to cause disruption and the financial means to procure these services, even if they do not have the capabilities to do so themselves. This has led to an entire market or shadow industry supporting the ransomware ecosystem, providing services such as selling access to corporate networks (through brokers responsible for initial access) or money laundering.[2] Today, there is a complex, international ecosystem, including ransomware operators, affiliates, and developers.[3] This model further fuels research and development in ransomware, with profits being ploughed back for this purpose, thereby reinforcing the business model of the ransomware "enterprise".

4. To effectively counter the ransomware threat and prevent the industry from further entrenching itself, it is critically important that countries address the ransomware problem as a **cross-border** and **cross-domain** challenge. It requires all countries to work together to deprive ransomware actors of their criminal profits, disrupt the ransomware business model, and improve our defences against ransomware attacks as a global alliance against the criminal actors. It also requires countries to take similar steps domestically to coordinate their cybersecurity, law enforcement, and financial regulatory agencies and support global cooperation. Both efforts are mutually reinforcing, and one cannot be effective without the other.

[2] It is rare that the ransomware creator, seller, user, and network perpetrator is the same entity; each provides a niche "service". It has therefore become very challenging to differentiate between these interdependent players and attribute malicious activities to them.

[3] Ransomware developers write the ransomware programme and sell it to ransomware operators. Ransomware operators then provide the Ransomware-as-a-Service (RaaS), while ransomware affiliates leverage this service and focus their efforts on spreading the ransomware by carrying out cyber-attacks. Operators typically recruit affiliates through closed-door channels or underground fora, and they will take a cut from the ransom pay-out. As the affiliates do the bulk of the work under the RaaS model, they also help operators diversify the risks of identification and arrest.

The Counter-Ransomware Task Force

5. To address a cross-domain and cross-border challenge, we must first have strong coordination across the whole of Government, to develop a coherent approach to tackle ransomware domestically and internationally. This was the impetus for the Counter-Ransomware Task Force (CRTF).

6. The CRTF was convened in January 2022. It was chaired by the Commissioner of Cybersecurity and Chief Executive of the Cyber Security Agency of Singapore (CSA) David Koh. The CRTF's membership comprised senior representatives from CSA, the Monetary Authority of Singapore (MAS), the Ministry of Home Affairs (MHA), the Singapore Police Force (SPF), the Ministry of Communications and Information (MCI), the Infocomm and Media Development Authority (IMDA), the Ministry of Defence (MINDEF) and the Government Technology Agency (GovTech), with supporting representatives from the Attorney-General's Chambers (AGC).

7. The CRTF's Terms of Reference (TOR) were to:

a. Develop policies, operational plans, and capabilities that the Government needs to improve the way we counter ransomware.

b. Arising from the policies, operational plans and capabilities developed in (a), determine the implementation route map for respective agencies to operationalise them.

c. Submit a Task Force report comprising findings and recommendations.

8. The CRTF met six times between January and September 2022, with work culminating in three key outcomes:

a. A consolidated understanding of the ransomware kill chain, upon which Government agencies can coordinate and develop counter-ransomware solutions;

b. The CRTF's recommendation on whether victims should pay ransom to ransomware actors; and

c. Recommended strategies for Singapore to pursue to curb ransomware attacks on Singapore entities and contribute to the global fight against ransomware.

The Ransomware Kill Chain

9. Understanding the attacker's logic is the first step to countering it. Thus, **the CRTF sought to develop a reference ransomware kill chain**, to set out how an attack takes place in cyberspace. (see Figure 1).

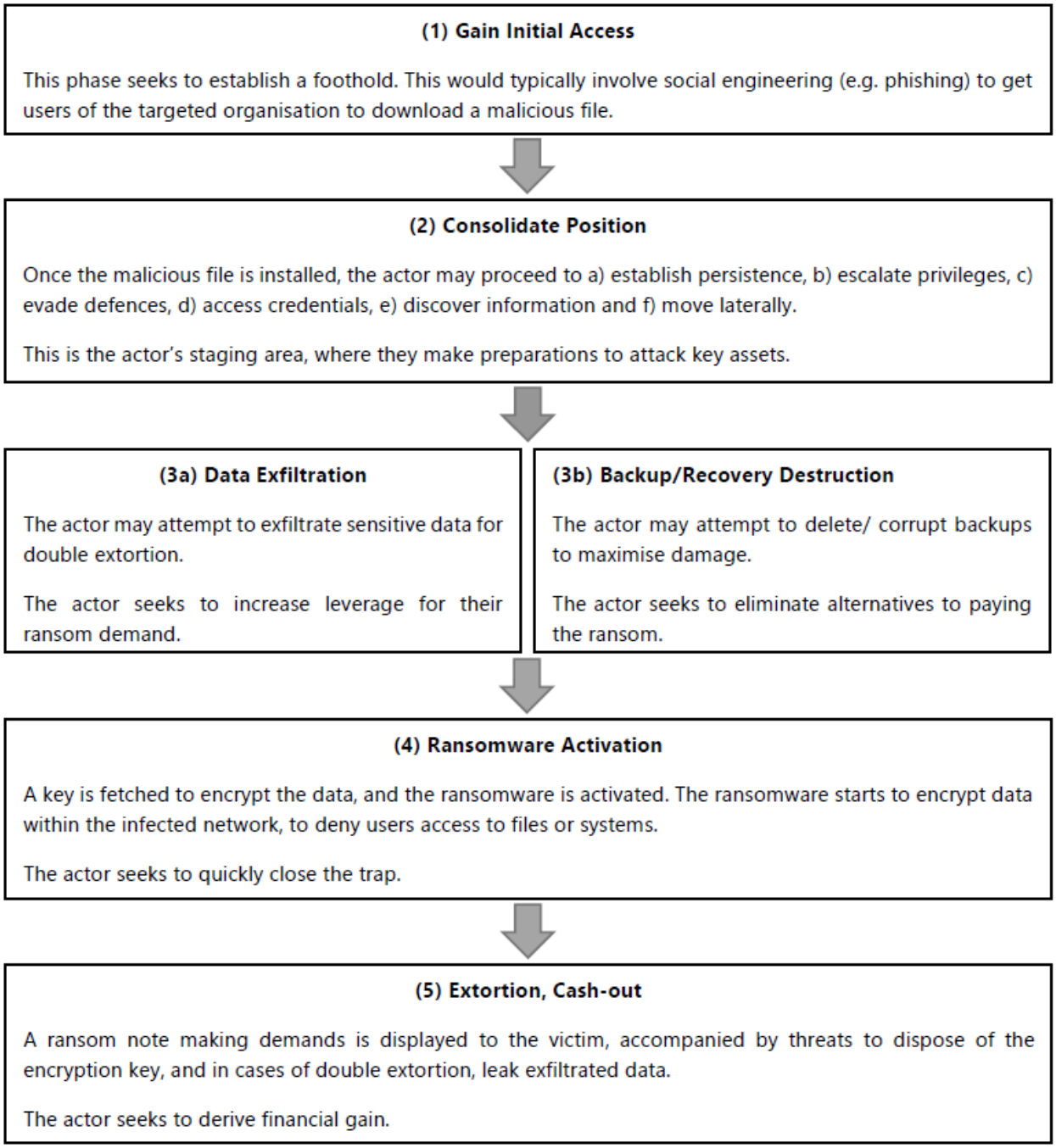

Figure 1: Reference Ransomware Kill Chain

10. The kill chain posits that there are five stages of a ransomware attack. The first three stages of the kill chain take place before the activation of the ransomware. This is when the attacker gains access to the targeted system, establishes a foothold within it and executes preparatory steps for the ransomware attack, such as exfiltrating data for double extortion or deleting existing backups to maximise damage to victim. During these stages, stealth is often a priority for the attackers, and attackers have been known to perform these steps months before activation. After the ransomware is activated, the ransomware works to encrypt identified data to deny users' access (stage four), and display the ransom note with the attacker's demands (stage five). These stages of the kill chain must be completed quickly, to constrain the victim's ability to remediate the attack.

11. Prevention is better than cure; thus, stopping the kill chain at stages one and two should be the priority. As these stages are similar to cyber kill chains associated with other, more typical cyberattacks, a primary focus should be to ramp up and improve existing measures to raise users and organisations' cybersecurity and resilience. Some technical measures can also be developed to minimise the chances of ransomware attackers getting past stage one, such as through the use of Protective Domain Name Service (pDNS) or other takedown measures. Takedown measures may also be effective past stage two and before activation; however, they can only be used for known malicious domains or campaigns.

12. After the ransomware has been activated, efforts must pivot to mitigation and remediation instead, such as through the employment of decryption keys and the activation of existing backups. While these measures allow victims to retrieve and/or restore data, instances of double extortion – where the attacker both encrypts the data and threatens to publicise sensitive information – renders them only partially effective at fully mitigating ransomware attacks.

13. **Ultimately, having a common reference model of a ransomware kill chain will allow countries to better understand each other, facilitate information sharing and benchmark counter-ransomware best practices and identify gaps in existing national measures.** International discussions on establishing a common understanding of the ransomware kill chain are beginning, and the CRTF recommends that Singapore keeps abreast of these discussions, contributes actively to the development of the common reference model, and updates our own understanding to ensure alignment.

Position on Paying Ransoms to Ransomware Attackers

14. **The ultimate goal of a ransomware attack is to obtain a ransom.** Attacks are designed to put pressure on victims to pay the ransom, by threatening consequences that the attackers bet would likely cost the company more than the ransom amount demanded. Allowing attackers to achieve their objective by paying the ransom fuels the ransomware problem. **Therefore, Singapore's national position is that the payment of ransoms to ransomware attackers is strongly discouraged.**

15. **The CRTF reviewed this position and concurs**. Obtaining a ransom is the objective of the ransomware attacker, and paying the ransom fuels the ransomware problem. Thus, the first objective of countering the ransomware problem must be to discourage victims, as far as possible, to not pay the ransom. The CRTF noted that in the event of an incident, paying the ransom does not guarantee the decryption of data or that data will not be published by the ransomware attacker. In fact, an organisation that has paid up before may also be identified as a "soft" target and be hit again. This position is in line with that of other countries.

16. The CRTF also noted that the payment of ransoms to ransomware attackers under certain circumstances could, depending on the facts, be in contravention of the Terrorism (Suppression of Financing) Act ("TSOFA") 2002, which criminalises the financing of terrorist acts, and recommends that Government agencies and owners of CII consider this risk, notifying CSA and SPF immediately in the event of a ransomware attack before any ransom payments are made.

Recommended Actions

17. To address the ransomware threat effectively, the CRTF recommends that the Government focus on four pillars of action:

> Pillar 1: **Strengthen defences** of high-risk targets (such as Government agencies, critical information infrastructure, and businesses) to make it harder for ransomware attackers to launch successful attacks.
>
> Pillar 2: **Disrupt the ransomware business model** to reduce the pay-off for ransomware attacks.
>
> Pillar 3: **Support recovery** so that victims of ransomware attacks do not feel pressured to pay the ransom, which fuels the ransomware industry.
>
> Pillar 4: **Work with international partners** to ensure a coordinated global approach to countering ransomware.

Pillar 1: Strengthen our Defences

18. Preventing a successful ransomware attack is paramount. As the ransomware kill chain illustrates, ransomware attackers must begin by gaining access to the victim's system and remaining undetected long enough to consolidate its position, exfiltrate data and destroy back-ups. This means that strong technical measures can prevent or disrupt a ransomware attack.

19. It is ultimately impossible to eliminate all cybersecurity risks, and trade-offs between security and performance must sometimes be taken. Thus, each organisation must take a risk-based approach to strike a balance between ease of operations and cybersecurity, so as to reduce the risks to a level acceptable to the organisation.

20. When defences are weak, we become soft targets to threat attackers. Raising the cyber posture of CII, Government agencies and companies is a form of protection, risk mitigation and deterrence. As a general guideline, the CRTF recommends looking into how the Government could better encourage organisations and enterprises to:

a. Create an inventory of all physical and logical assets that make up the system and identify assets that are important and critical. These important and critical assets should be subjected to more stringent security measures compared to all other assets.

b. Implement risk-mitigation measures such as:

i. Credential management. A sound credential management policy helps to prevent unauthorised access. CII organisations should properly implement multi-factor authentication on key assets and manage changes and adjustments (e.g. lost passwords and personnel changes) to prevent unauthorised access.

ii. Network segregation and segmentation. Enterprise networks should be segregated according to each segment's security and risk levels, thus preventing key assets from being connected to enterprise networks.

iii. Backup and restoration plan. Periodic backups should be performed to ensure that key assets can be recovered in the event of a ransomware attack. To prevent ransomware attackers from deleting or encrypting backups, backups should be kept offline or disconnected from the organisation's network.

21. Although ransomware attackers tend to attack opportunistically and any person or organisation can be a potential target, the CRTF recognised that due attention should be given to two groups:

a. Critical Information Infrastructure (CII), as these could be especially attractive targets due to attackers assuming that disruptions to essential services would place great pressure on the owners to pay the ransom.

b. Small and Medium Enterprise (SMEs), which may be particularly vulnerable as they face constraints in resources and capabilities in instituting the appropriate cybersecurity and risk management measures.

22. For CII, the CRTF reviewed the Cybersecurity Code of Practice, which was recently revised in July 2022, and agreed that it provided adequate guidance for owners of CII on the appropriate risk identification and mitigation measures. **This CCOP will be regularly updated to ensure that it remains fit-for-purpose.**

23. For SMEs, the CRTF noted that there are initiatives in place to guide SMEs and help them benchmark their cybersecurity practices, such as the **Cybersecurity Toolkit**[4]

[4] The Cybersecurity Toolkit for SMEs provides information on cybersecurity issues and threats to enable organisations to adopt cybersecurity measures pertinent to their job roles, such as making business leaders bilingual in technical and strategic language, IT teams knowledgeable on how to best implement cybersecurity within their organisation, and employees able to adopt tips to address common threats such as phishing.

and the **SG Cyber Essentials and Trust Marks**.[5] **Thus, the CRTF recommends looking into developing incentives and support schemes to improve awareness and adoption of these existing initiatives.**

24. In addition to improving enterprise cybersecurity, **the CRTF also suggests looking into ecosystem-level interventions:**

a. Implementing Protective Domain Name Service (pDNS) as a form of "upstream defence", to prevent known malicious attackers from reaching internet users.

b. Supporting the development of tools (e.g. firmware) that could help detect ransomware, defeat unauthorised encryption, or otherwise protect digital assets from ransomware to prevent the successful execution of the ransomware kill chain.

Pillar 2: Disrupt the Ransomware Business Model

25. While the CRTF recognised the importance of getting organisations and enterprises to better protect themselves, there is a need to reduce, if not eliminate, the profitability of ransomware attacks. This is to neutralise the business logic of ransomware. Ransomware attacks continue to grow because there is a "high return on investment". The low barrier to entry due to the RaaS model places ransomware capabilities in the hands of anyone who has the financial means to procure RaaS. As long as ransomware attackers can be confident of eliciting a ransom and evading law enforcement, the crime will pay off. As such, the CRTF recommends:

a. Discouraging ransom payments to reduce the profit that ransomware attackers can expect from setting up ransomware attacks; and

b. Tracing the illicit flows of assets paid in ransom more effectively to reduce the likelihood of ransomware attackers being able to abscond with ransom payments.

A. Discouraging ransom payments

26. Ransomware attacks are designed such that paying the ransom will likely be the least painful option for a business that has not taken adequate steps to mitigate the damage of a ransomware attack. Businesses' likelihood of paying the ransom can be further exacerbated by the availability of cyber insurance policies that specifically include

[5] The Cyber Essential Mark is a cybersecurity certification for organisations just beginning to implement cybersecurity measures, while the Cyber Trust Mark offers certification for organisations with more extensive digitalised business operations. Both Marks recognise organisations for good cybersecurity practices.

coverage for the payment of ransoms, which can make paying a preferred option to victim organisations.

27. **The CRTF is of the view that it would be timely for the Government to re-publish advisories on ransom payments, to strongly emphasise that the Government does not condone the payment of ransoms and highlight the risks and implications of doing so.**

28. **The CRTF also recommends studying the implications of cyber insurance policies that include coverage of ransom payments on the ransomware industry, and the potential impact if such coverage is disallowed.** There are preliminary indications that policy holders are more likely to pay ransoms if there is insurance coverage,[6] and that such payments play a part in fueling the ransomware industry.

B. Tracing the illicit flows of assets paid in ransom more effectively

29. Ransomware attackers often demand that ransoms be paid in cryptocurrency, then obscure cryptocurrency trails through the use "cryptocurrency mixers" or "cross-chain bridges" to convert ransoms into different cryptocurrencies or privacy-centric cryptocurrencies. Some Virtual Asset Service Providers (VASPs) also operate in multiple jurisdictions without a clear domicile, making it difficult to identify whether specific illicit transactions are with a digital wallet hosted locally or overseas, impeding tracing efforts. In addition, the growing use of private wallets and decentralised finance (DeFi) further complicate the tracing of the flow of illicit payments.

30. **The CRTF recommends considering making it mandatory for organisations to report the payment of ransoms.** Such information is necessary for the Government to be able to trace these illicit financial flows, claw back ransom payments, and ultimately bring ransomware attackers to justice.

31. **The Government will also look into augmenting our tracing capabilities by tapping on public-private partnerships.** Ransom payment tracing is currently limited by the capabilities of commercial cryptocurrency analysis tools, as well as the Government's own in-house capabilities to conduct in-depth investigations. Given blockchain solution providers' expertise in blockchain protocols and access to extensive data around the world, it may be more effective to engage these providers for forensic cryptocurrency tracing and joint investigations to enhance the Government's ability to link ransom payments to ransomware operators, with potential exceptions for cases concerning highly sensitive or classified entities.

---

[6] A 2020 global survey commissioned by Sophos of 1,823 companies, government, health systems and other organisations hit by ransomware found that 32 percent of organisations with cyber insurance against ransomware paid the ransom, while only 15 percent of those without it paid.

Pillar 3: Support Recovery

32. To effectively counter ransomware, the cooperation of victim organisations is key. Victim organisations must support the effort by not paying ransoms to ransomware attackers as much as possible. Their timely reporting of attacks and any payment made is also necessary for law enforcement to conduct effective investigations and to improve our overall understanding of ransomware criminal operations for the future.

33. Providing genuine and effective support for victims to recover from ransomware attacks is the only way to encourage victims' cooperation in this area. The CRTF recognises that victims' reluctance to report ransomware attacks is a real concern, either due to fear of reputational damage or being penalised for cybersecurity breaches. Ransomware victims should not feel as if they are being punished for doing the right thing by reporting an attack and not paying the ransom.

34. The CRTF recommends the following measures:

a. Providing resources to victims to help recover from ransomware attacks; and

b. Encouraging cyber insurance as a risk management practice.

A. Providing resources to victims to help recover from ransomware attacks

35. **The CRTF recommends creating a one-stop portal for organisations to access all ransomware-related resources, aimed at victims of ransomware attacks seeking recovery support.** The portal will provide links to resources, such as decryption keys and response checklists, that could assist them in recovery efforts after a ransomware attack. One such resource is Europol's *nomoreransom.org*, a website where public and private entities around the world regularly share new decryption tools for the latest strain of ransomware; its tools are free to all. As recovery support includes preparing victims to prevent another ransomware attack, the portal could also provide resources on preventative measures, such as the Cyber Essentials and Global Cyber Alliance cybersecurity toolkits, as well as alerts and advisories.

B. Encouraging cyber insurance as a risk management practice

36. **The CRTF also recommends exploring levers to increase the take up rate of cyber insurance amongst CIIOs and SMEs**, while the impact of covering ransom payments (at Paragraph 29) is being studied**.** Even if ransom payments are not covered, obtaining cyber insurance coverage for other potential costs arising from a cyber incident is still a useful risk management practice as it allows an organisation to transfer and/or share the risks arising from a cyber incident with private commercial insurance companies. Cyber incident related costs such as business income loss and the expenses

of incident response can be claimed against the cyber insurance policy, where contractual criterion has been met. Such cyber insurance can also incentivise organisations to adopt better cybersecurity measures to meet the underwriting requirements. The CRTF also recommends looking into developing a guide on cyber insurance for enterprises and potentially onboarding cyber insurers with curated cyber insurance packages to minimise discovery costs for enterprises.

Pillar 4: Work with International Partners

37. Given the borderless nature of the ransomware threat, nothing that Singapore does on our own, within our jurisdiction, will be sufficient to effectively counter ransomware. Thus, it is **paramount to the counter ransomware effort that we support and contribute to a coordinated global effort to address the ransomware threat.**

38. The CRTF is of the view that Singapore must:

a. Support the development of best practices in information sharing, law enforcement and financial regulation, to improve cross-border coordination;

b. Drive the adoption of these best practices, so that collectively, we deny safe havens to ransomware attackers;

c. Contribute to capacity and capability development, so that there are no "weak links" amongst states that ransomware attackers can take advantage of.

39. **The international conversation on countering ransomware is gaining traction**, as many other states are also growing increasingly cognisant of the threat posed by ransomware. While there has been some push for a cross-domain platform (e.g. the US-led Counter Ransomware Initiative), many of these conversations are taking place at existing, domain-specific platforms, each fronted by the respective domain-leads within the Government. These include:

a. United Nations Ad-Hoc Committee on Cybercrime (AHC);

b. Financial Action Task Force (FATF);

c. INTERPOL, EUROPOL, ASEANAPOL; and

d. International Association of Insurance Supervisors (IAIS).

40. To be effective, the Government must have a **coordinated strategy and approach across the various platforms**, so that the various agencies representing

Singapore at these discussions are **cognisant of Singapore's collective offensives and defensives in the fight against ransomware**, and are **positioned to seize relevant opportunities within their domains**, to forward the counter-ransomware agenda more effectively.

41. The CRTF identified three specific areas in which Singapore should double down on and contribute to efforts to foster international cooperation:

a. Law Enforcement. To bring ransomware attackers to justice and deny these criminals safe havens, **the CRTF recommends exploring ways to expedite cross-border law enforcement collaboration on a bilateral or plurilateral basis for information exchange and interdiction of ransom payments.** Current processes to track down criminals and interdict payments across borders are slow and inefficient, as foreign VASPs are often constrained by the laws and regulations of their own jurisdictions. Some foreign VASPs are only willing to disclose information on a court order, which may necessitate making a Mutual Legal Assistance (MLA) request to that jurisdiction. The process of getting a foreign jurisdiction to act may be tedious and long-drawn, especially where quick action is needed to prevent dissipation of the proceeds of ransomware attacks, and there is often no guarantee of useful returns despite the effort undertaken. An international framework for processing and acting on these requests would speed up and smoothen cross-border law enforcement efforts.

b. Anti-Money Laundering Measures. The regulatory loopholes and gaps allowing ransomware actors to launder their ill-gotten gains across borders are not new, but the ransomware threat has made evident the need to ensure that these illicit financial flows can be traced and the abuse of virtual assets stopped. **The CRTF recommends that Singapore continues to work with international counterparts towards timely and consistent implementation of FATF standards on combating money laundering and the financing of terrorism and proliferation.**

c. Discouraging ransom payments. Without international alignment on the insurance policies covering ransom payments, any attempt to discourage these within our domestic market will be ineffective as businesses can easily turn to insurance providers overseas to buy insurance policies. **The CRTF thus recommends working with international partners to study the effects of insurance policies covering ransom payments on the ransomware industry**.

Conclusion

42. The Counter-Ransomware Task Force Report will serve as a blueprint to guide Singapore's efforts to foster a resilient and secure cyber environment, domestically and internationally, to counter the growing ransomware threat. These recommendations will also form the basis for improved cross-domain collaboration within the Government on this issue. As we expect the ransomware threat to become ever more sophisticated, it is important for the Government to ensure that we have the right defences in place to protect our systems and to respond to attacks robustly. Our nation's resilience against ransomware threats and overall cybersecurity posture will also undergird our growing digital economy by securing digital trade. However, given the scale and severity of the ransomware threat, Singapore cannot achieve these objectives alone. It is thus imperative that we also work with other countries to contain the threat posed by ransomware attacks.

———————