UK FINANCE

THE RISE IN RANSOMWARE AND GROWING GOVERNMENT CONCERN

Banking and finance sector position

May 2022

EXECUTIVE SUMMARY

Ransomware represents one of the most significant and growing international cyber threats, with serious economic, security and public safety consequences. Ransomware is no more a complex crime type – the full lifecycle becoming readily available to novices to take advantage, through areas such as Ransomware as a Service. In some cases, key threat actors operate from safe havens with payments made in largely unregulated cryptocurrency.

The UK government continues to grapple with the impact of ransomware attacks on critical national infrastructure and more broadly, across sectors within the UK, as well as the international implication of cyber threats on the UK economy. In late 2021, the G7 Cyber Expert Group made a call to action to member states to identify and disrupt ransomware criminal organisations and networks, calling out the importance of responding swiftly in order to hold these networks accountable for their actions. This is built on existing initiatives, such as the International Counter Ransomware Initiative, which harnesses expertise from across the G7 with the goal to find practical policy solutions, develop proposals on technical assistance, advance policy cooperation and raise public awareness.

The focus of these initiatives include:

- improved national resilience;
- expansion of national preparedness;
- disruption of the criminal eco system and undermining the ransomware business model;
- disruption and deterrence of cyber criminals.

Similarly, we can reference the work done by the Ransomware Taskforce, a part of the Institute for Security and Technology, on a comprehensive framework for action in response to the rise in ransomware. In this it highlights the need for collective effort to mitigate the ransomware scourge. In reference to the banking and finance sector, we are aware that the impact of ransomware attacks within an organisation can severely disrupt business processes, compromise of, and access to, critical data. We welcome action across the UK government on ransomware and the opportunity to recommend and support activities which are important to the banking and finance sector.

UK Finance, on behalf of its members, calls on the UK authorities to focus on ransomware criminals in the following key areas:

1. In the short term, aggressive action in the form of sanctions as well as better communications and reporting processes to improve knowledge of threats and scenarios across the UK.
2. Expansion of regulations to cover non-bank entities that facilitate the ransomware business model, including money servicing businesses and crypto exchanges.
3. In the longer term, considerations on the use of the right legislation and standards setting to provide a sustained approach to managing the use of cryptocurrencies in cyber-attacks and fraud.

The growing concern with cryptocurrencies

The primary motive for ransomware is the prospect of financial gain. Ransomware attackers, if successful, often receive payment in cryptocurrency, which they then seek to launder and "cash out" of the crypto ecosystem. Attackers may also use cryptocurrency to procure goods and services to support their activities. The more the government and regulators can do to restrict the use of cryptocurrencies and to minimise the likely financial reward of a ransomware attack, the lesser the incentive for criminals to carry out such attacks.

The ability to sanction crypto exchanges goes beyond the remit of the UK authorities. Further thinking around legislation or guidelines will need to consider and include all regulations meant to limit criminality in the financial system, in addition to the extent that said legislation can cover sanctions. In addition, further consideration is needed on the development of technical requirements such as ledgers, which make it easy to track and record the use of an identifiable token in cryptocurrency transactions.

While we continue to consider the extent to which sanctions can be used to limit these attacks, there is a need to pursue mechanisms as part of the aggressive action, working closely with the private sector in tackling this issue.

Banking and finance sector recommendations

1. **Better regulatory standards and rules in the use of cryptocurrencies**

There is a need for stronger regulatory standards around the use of cryptocurrencies to facilitate illicit activity, as well as clearly defined rules for crypto exchanges and virtual asset service providers. The use of information sharing on clean funds in economic crime could be introduced in the event of a ransom payment for a ransomware attack. In alignment with the National Economic Crime Centre plans, we welcome the push for stronger enforcement powers following a ransomware attack in the following areas:

- designation of powers to law enforcement to freeze and/or seize all types of crypto assets;
- sanctions or other public sector powers by the UK to stop payments to specific crypto asset service providers, where there is a high risk of economic crime and/or they are not cooperating with requests from UK law enforcement or regulators.

2. **Greater financial services involvement in legislation and standard setting**

An action that can have a significant impact is greater UK involvement in standard setting. Although the impact of this action may be long term, it sets the base for longer-term deterrence to threat actors. In addition, on legislation, particularly on sanctions, there is a need for greater clarity and understanding of the relevant policy and legal tools to be used in setting the legislation.

We welcome banking and finance sector involvement in the online fraud steering group progressing action in the following areas:

- actions for an industry group to develop proposals for using APIs to facilitate information exchange;
- appropriate cross-sector industry forums for private to private communication where required;
- provision of private to private education and awareness for KYC/AML processes for crypto exchanges and virtual asset service provider (VASP) clients.

3. Greater financial services involvement in the global ransomware taskforce (RTF)

The RTF released its 2022 comprehensive framework to combat ransomware. We welcome the defined framework and fully support the drive to ensuring sustained engagement across UK government, law enforcement and the private sector initiatives feeding into the RTF. We further highlight opportunities, below, to provide financial services support across the various workstreams put in place to deliver this framework.

On activities to deter ransomware criminals: It is important to acknowledge the need for global operational collaboration in the action on ransomware criminals through the cryptocurrency group, cyber insurance group and ransomware controls group. We highlight the opportunity to provide recommendations and to support through the G7 Cyber Expert Group focused on ransomware.

On activities to disrupt the payments systems and infrastructure: The ransomware incident response network is focused on defining actions to disrupt infrastructure used to facilitate payments and establish a global network of ransomware investigation hubs with increased government to private intelligence sharing. UK Finance would welcome the opportunity to participate in the UK cross-Whitehall ransomware group or other of its kind and to share sector experience and recommendations with the network.

On activities to prepare and improve awareness for ransomware mitigation, response, and recovery: UK Finance would welcome the opportunity to be positioned as a regional coordination base working closely with the National Cyber Security Centre (NCSC) and the Financial Sector Cyber Collaboration Centre (FSCCC) where possible, to support the ongoing workstreams tasked with delivering standards, frameworks and campaigns to improve awareness and disrupt ransomware activities. The FSCCC is a public, private partnership that identifies, investigates, monitors, and coordinates incident response on potential systemic threats to the banking and finance sector.

On activities to develop emergency response and incident response network with government and authorities: The importance of cross-sectoral communication is a significant aspect of proposed actions in response to the rise in ransomware. The banking and finance Sector Response Framework (SRF) provides an effective framework for sector level coordination, decision making and communication during a major incident, at both a strategic and tactical (modular) level within the UK banking and finance sector.

As seen in the Take 5 campaign and in our position as the trade association representing the banking and financial services sector, UK Finance is best placed to support the societal impact and awareness campaigns.

Furthermore, UK Finance's participation in the future of finance intelligence sharing group connected into the global coalition to fight financial crime provides an opportunity for banking and finance sector input into awareness campaigns.

4. **Guidelines/principles for dealing with ransomware and the cyber insurance sector**

It is important to highlight the relationship between cyber insurance and ransomware and the role the cyber insurance sector plays. Our position remains that paying ransoms should be the last resort and the government's focus must be to understand the impact of ransomware on government, law enforcement and the economy, working in collaboration with insurance-focused trade associations and marketplaces. We welcome the key questions highlighted in the ongoing project by RUSI on the role of cyber insurance in ransomware, which calls out the opportunity for public-private partnerships between the insurance industry and the government.

Conclusion

While the sector welcomes government action to improve our understanding of the threats, crypto, payments, role of insurers and impact of ransomware attacks on the sector, action is required by the UK government and regulators in these areas in order to have an impact on the cyber threat landscape now and in the future. The importance of clarity in the government and authorities' priority areas cannot be overstated, as it provides a cross-sectoral roadmap of how we can play a part in the actions to limit criminality of ransomware attacks through the use of cryptocurrencies.

The UK banking and finance sector is keen to engage on what needs to be done to fight the ransomware epidemic, and to limit the use of cryptocurrencies in ransomware criminality and the wider crypto ecosystem – both in order to protect the industry but also other sectors who are our clients.

AUTHORS:

Ian Burgess
Director, Cyber and Third Party Risk,
UK Finance

Oge Udensi
Principal, Cybersecurity,
UK Finance