EUROPEAN CENTRAL BANK

EUROSYSTEM

Ransomware: oversight perspective for financial market infrastructures

As the ransomware threat for the financial sector remains at a high level for a protracted period of time, international initiatives have been established to mitigate possible ransomware attacks and their impact. In this light, the G7 published the eight Fundamental elements of ransomware resilience (G7 FE ransomware)[1] in October 2022.

The current document places the eight fundamental elements in an oversight perspective, by cross-referencing the CPMI-IOSCO Guidance on cyber resilience (CPMI-IOSCO Guidance), the Eurosystem Cyber Resilience Oversight Expectations (CROE), the TIBER-EU framework and other related G7 FE publications where relevant. The purpose of this document is to provide overseers with a brief overview of relevant European[2] documentation.

1. Defining ransomware attacks

Ransomware is a type of malware that primarily encrypts data. Reverting the encryption can only be achieved with a so-called decryption key, which attackers offer in return for a ransom – usually in crypto assets. This type of attack is mainly used by criminals of different background and motivation to cause disruption or for monetary gain, with average ransom demands continuously rising[3]. When ransomware is released on a system, the functioning of said system is obstructed as the data it uses become unreadable. Once encrypted, the contents of files and databases become obfuscated, destroying file paths as well. A successful ransomware attack has a fundamental impact on the availability, confidentiality and integrity of data, severely impacting an entity's ability to operate.

Attack process

- Prominent attack vectors include the use of spear phishing, compromise of internet-facing systems[4] or using an initial access broker[5]. Targeting is often opportunistic, for example through the use of newly discovered software vulnerabilities.
- Once inside a company's network, the ransomware attackers may conduct research on the entity's characteristics, enlarging their chances for a maximum pay-out. Depending on the size and turnover of the victim, the requested amount can reach millions, often to be paid in crypto-assets.
- The victim is pressured to pay the ransom, as this may be considered by the victim as a cheaper and faster solution than full system restoration. Before encryption, attackers often exfiltrate large amounts of sensitive data out of the company's network. The leaked data may then be used to further pressure the entity, threatening to release the sensitive data online. This double,

[1] The G7 FE Ransomware document was published after the October 2020 G7 Statement, and is based on the G7 Fundamental Elements of Cybersecurity (G7 FE CS) by contextualizing the specificities of ransomware threats.
[2] Further background by FSB (2020) 'Effective Practices for Cyber Incident Response & Recovery'.
[3] CoveWare, 'Fewer Ransomware Victims Pay, as Median Ransom Falls in Q2 2022', 28 July 2022, https://www.coveware.com/blog/2022/7/27/fewer-ransomware-victims-pay-as-medium-ransom-falls-in-q2-2022, accessed 23 February 2022.
[4] Compromise of internet facing systems generally happens through a software vulnerability in said systems, allowing malicious actors to exploit weaknesses and enter the victims' network.
[5] An initial access broker is a malicious actor that sells the initial access to a victims' network for other actors to further exploit.

or even triple extortion – where even the entity's customers are contacted by threat actors – has become common practice.
- Ransomware-as-a-Service (RaaS) enables even unskilled attackers to conduct these types of attacks.
- Payment of the ransom supports the criminal business model, but does not guarantee that the attackers will provide the decryption keys, delete any exfiltrated data or that a full data restoration will be successful.

2. Application of the G7 Fundamental Elements

2.1 G7 FE: Cybersecurity Strategy and Framework

Incorporate ransomware resilience within the entity's overall cybersecurity strategy and framework.

Many ransomware attacks leverage well known security problems and attack methods, often benefiting from an entity's inadequate cyber habits. Adequate cyber hygiene practices[6] therefore effectively reduce the chance of a successful ransomware attack. What is deemed 'adequate' depends on the entity's context and threat landscape. To guide financial institutions, the CPMI-IOSCO Guidance and CROE provide concrete elements on how to improve and build cybersecurity and resilience.

Although not mutually exclusive, resilience against ransomware is generally built, not bought. This means that a financial entity cannot achieve resilience by simply purchasing cyber solutions: it has to invest to build resilient systems and create staff awareness. To allocate the necessary resources, the board and senior management should approve and endorse the entity's cybersecurity strategy.

Regularly conducting crisis management exercises and red-team tests – such as via the TIBER-EU framework – help to build a resilient organisation and foster board involvement. These elements should be included in the cyber resilience strategy of the entity, with attention for the broader ecosystem. Setting a comprehensive exercising program is described comprehensively in the G7 FE of Cyber Exercise Programmes (G7 FE CEP). Critical third parties may fall victim to a ransomware attack too[7], indirectly impacting the financial entity. To improve ecosystem resilience, third parties should therefore be a part of the entity's cyber resilience strategy.

Relevant provisions:
- CPMI-IOSCO Guidance § 2.2, 7.2
- CROE § 2.1.2, 2.6.1

2.2 G7 FE: Governance

Ensure effective coordination for the broad organizational impacts of ransomware through effective governance structures.

The impact of a ransomware attack is not confined to technical aspects of an organisation, but severely impacts a broad selection of (critical) business functions, such as operations, legal and regulatory compliance or public affairs. Therefore, an entity needs to prepare for cross-organizational involvement, prepare business continuity plans and communication plans. Because of this broad potential impact, a

[6] The European Union Agency for Cybersecurity (ENISA) has published a useful report on the leading cyber hygiene programs across the EU.
[7] In this light, solid end point security is crucial for the overall payment system, as described in the 2018 CPMI publication 'Reducing the risk of wholesale payments fraud related to endpoint security'.

strong cyber-awareness culture must be promoted, with a leading role for the board and senior management.

In a worst-case scenario, data and systems could be completely unavailable – even if a ransom were paid – through faulty decryption software or attackers not providing a decryption key. In essence, the entity may be unable to resume operations for a prolonged period of time, which could threaten its existence. Entities should assess the possible impact of such a scenario and take appropriate measures. As outlined in the G7 FE Ransomware, G7 countries generally discourage ransom payments, and note that these payments may violate (inter)national regulations or industry standards.

Relevant provisions:
- CPMI-IOSCO Guidance § 2.3
- CROE § 2.1.2.2

2.3 G7 FE: Risk & control assessment

Ensure the application of controls to address ransomware risk.

To properly assess ransomware risk, entities need to identify their critical functions, the key roles and assets, including the ones that depend on third parties. Automated tools may assist in identifying critical links, but a thorough cyber risk assessment for third parties and their criticality is indispensable – as for instance defined in the G7 Fundamental Elements for third party cyber risk (G7 FE 3rd party risk, see Box 1 below).

Box 1: Sector resilience & G7 FE of 3rd party risk

Sector resilience can only be achieved by engaging the whole ecosystem. The financial sector is interconnected to a multitude of third parties, effectively enlarging the attack surface. As described in the G7 Fundamental Elements for third party cyber risk, the involvement of third parties starts with their identification and assessing their criticality. In the case of ransomware, third parties may have to stop services for a prolonged period of time, possibly impacting core financial services as well.

Institutions may opt for cyber insurance to cover potential damages of a ransomware attack. As part of the policy, cyber insurers will require the entity to adhere to the highest cybersecurity standards and practices, effectively supporting cybersecurity. However, insurance policies are not a substitute for strong cyber hygiene practices and effective counter-ransomware planning.

Relevant provisions:
- CPMI-IOSCO Guidance § 3.2, 3.3, 4.2, 4.3
- CROE § 2.2.2, 2.3.2.1
- G7 FE 3rd party risk: Element 2

Box 2: The paradox of cyber insurance

There are clear advantages to cyber insurance, especially regarding ransomware. Insurance can support an entity's resilience, requiring solid cyber security practices as part of its policy. However, entities may rely on the insurance and reduce their efforts. If attackers know that an institution has cyber insurance, they often demand a higher ransom. Entities with insurance may therefore be a more attractive target. From an insurers' perspective, the lengthy restoration of systems and data, with accompanying business impact, may be much more costly to reimburse than paying a ransom. Ransom pay-outs by insurers could thus promote the ransomware criminal business model: the attacks prove to be worthwhile, instigating more ransomware attacks[8]. More attacks, in turn, would lead to a higher request for insurance, creating a vicious circle.

2.4 G7 FE: Monitoring

Monitor systems for signs of potential ransomware activity.

Financial infrastructures should develop the capabilities to detect anomalous activities. Based on the 'in-depth defense' security principle, entities should use a multi-layered network defence approach, combining multiple levels of security controls, instead of focussing solely on a single, 'outside perimeter' control. Strong Security Operation Centre (SOC) capabilities, equipped with intrusion, detection and security information and event management (SIEM) systems, can identify malicious behaviour in an entities' network and systems, and detect a potential ransomware threat.

(A)typical behaviour

Ransomware attacks usually show and follow known patterns – and have specific characteristics: e.g., events such as unusual user activity or the exfiltration of large data flows are commonly the precursor to the actual initiation of the encryption. Recognizing relevant technical indicators[9] – enabled through the use of cyber threat intelligence – thereby supports an adequate and timely response.

Relevant provisions:

- CPMI-IOSCO Guidance § 5.2, 8.2, 8.3
- CROE § 2.4.2, 2.7.2
- TIBER-EU Framework § 2.5, 8.5

2.5 G7 FE: Response

Implement established plans in response to ransomware incidents.

An effective ransomware response requires a systematic, multi-level approach, as defined in the G7 Fundamental Elements of Cybersecurity (G7 FE CS). Tested cyber resilience incident management, established cross-organizational plans with rapid communication and forensic readiness are indispensable for a quick ransomware response. Continuity plans should incorporate the impact of a ransomware attack for the entity's ecosystem.

If a financial entity were hit by a successful ransomware attack, swift professional help is of the utmost importance. Entities should therefore contact and ensure professional incident response capabilities in

[8] "Cyber Insurance and the Cyber Security Challenge", *MacColl*, *Nurse*, *Sullivan*, RUSI Occasional Paper, June 2021, p. 38-40, found at: https://static.rusi.org/247-op-cyber-insurance-fwv.pdf. Last visited: 2 February 2023.
[9] For example, the use of the Windows Command Shell, Scheduled Tasks and attempts to achieve 'credential dumping' are common indicators for ransomware attacks. Indicators can be obtained from open sources and commercial vendors.

advance, to help in the case of a ransomware attack. Established communication with public authorities, such as the respective national central bank, relevant authorities or possibly national cyber security centres, may help in responding timely to an incident. Experienced incident response teams (in-house or external) can limit the negative effects of ransomware and – if necessary – negotiate with ransomware attackers.

Relevant provisions:
- CPMI-IOSCO Guidance § 6.2, 6.4, 7.3
- CROE § 2.5.2
- G7 FE CS: Element 5
- G7 FE 3rd party risk: Element 3

2.6 G7 FE: Recovery

Take steps to restore capabilities that may have been impaired by a ransomware incident.

Even in case of a successful ransomware attack, the effects can be largely mitigated with adequate back-ups. Note that back-ups need to be recent to be of use, whereas restoring systems with the use of backups needs to be practiced regularly. The task is complex, and successful restoration of all systems can take several days to weeks – even with the right backups. Such restoration requires alignment with interconnected systems and processes of other entities within the financial ecosystem, which demands stakeholders to ensure a coordinated reconciliation[10].

Safeguarding data integrity requires multiple aspects to be taken care of, especially in the case of ransomware. Initial network infection may have taken place months before the actual attack – calling for thorough root cause analysis. Moreover, attackers may actively try to circumvent back-up strategies, requiring these strategies to be resilient. Storing back-ups at segregated, alternate sites with a lower risk-profile and stringent protective measures is therefore highly recommended.

If the entity choses to pay and would receive a functioning decryption key, the problems may not simply disappear. The success of retrieving the data largely depends on the quality of the attacker's decryption software, which often appears to be disappointing. Moreover, data links and file paths may be disturbed by the malware. This could leave the attacked entity with an unsorted data-dump, which takes tremendous efforts to restore.

Relevant provisions:
- CPMI-IOSCO Guidance § 6.2, 6.3.2
- CROE § 2.5.2.2

2.7 G7 FE: Information sharing

Exchange data, information, and/or knowledge about ransomware incidents and trends with internal and external partners.

After being targeted by a ransomware attack, the financial entity will need to inform law enforcement and supervisory authorities immediately. Through the aggregation of data, law enforcement will be able to combat ransomware more effectively. Noteworthy is the project nomoreransom.org, which provides decryption tools for many ransomware strings and offers useful advice. Authorities may be able to guide and help the entity through the recovery process.

[10] A conclusion of the December 2018 UNITAS Crisis communication exercise report, found at: https://www.ecb.europa.eu/pub/pdf/other/ecb.unitasreport201812.en.pdf. Last visited: 10 May 2023.

The entity may also wish to disseminate information of the ransomware attack to trusted and established information sharing initiatives, whenever possible. An example of such an initiative is CIISI-EU – the threat intelligence and information sharing initiative, established by the ECB Euro Cyber Resilience Board for pan-European financial infrastructures (ECRB)[11]. These types of initiatives provide a platform to share information, lessons learned, and furthering awareness of counterparts. Sharing cyber threat intelligence more broadly helps each entity to assess the threat landscape and to proactively manage cyber risk, by identifying trends and relevant threat actors.

Relevant provisions:

- CPMI-IOSCO Guidance § 8.2, 8.3
- CROE § 2.7.2.1, 2.7.2.2
- G7 FE CS: Element 7
- G7 FE 3rd party risk: Element 5

Box 3: nomoreransom.org

Europol, in cooperation with national law enforcement services and IT security partners, maintains a project to provide ransomware victims with free decryption tools. This is made possible by thoroughly analysing and 'cracking' different ransomware strings, exploiting weaknesses in the malware. As long as ransomware operations remain profitable, financial entities will be targeted. Adequate information sharing therefore enables this project to counter ransomware attacks in a broad sense, as it disrupts the criminal business model.

2.8 G7 FE: Continuous learning

Increase ransomware resilience by learning from past incidents.

After a ransomware attack, the financial entity needs to undertake root cause analysis and extract lessons from the attack and possible incident. The entity should be able to learn from similar incidents affecting its peers and broader ecosystem, by building and participating in information sharing links.

The entity should test its response and recovery capabilities utilising ransomware scenarios to continuously evolve its capabilities. TIBER-EU tests provide the opportunity to test the resilience of the entity under a controlled hacking exercise, to uncover areas of improvement in protection and detection.

Relevant provisions:

- CPMI-IOSCO Guidance § 9.2
- CROE § 2.8
- G7 FE CS: Element 8
- G7 FE CEP
- TIBER-EU Framework § 10.2 – 10.6

Box 4: TLPT: Simulating ransomware attacks

TIBER-EU is the European framework for threat intelligence-based ethical red-teaming. Core financial entities, threat intelligence providers, red-team providers and authorities work together – to test and improve the entities' cyber resilience by carrying out a controlled cyberattack. TIBER-EU tests mimic the tactics, techniques, and procedures of real-life threat actors, based on tailor-made threat intelligence. Ransomware scenarios are therefore frequently part of TIBER tests. The TIBER framework offers a different approach than the classic control-based assessments, offering the entity a true opportunity to assess its resilience against real-life ransomware attacks. After all, the only way to assess resilience is to test it. Experiences gathered in TIBER tests generate useful learnings and findings, strengthening the tested entities.

[11] https://www.ecb.europa.eu/paym/groups/euro-cyber-board/html/index.en.html