G-7 FUNDAMENTAL ELEMENTS FOR THREAT-LED PENETRATION TESTING

Executive Summary

In light of the increasing sophistication and persistence of cyber risks, which can threaten to disrupt our interconnected global financial systems, the G-7 continues to promote the development of frameworks to enhance public and private sector approaches to strengthening cyber resilience of critical entities in the financial system following its publication in 2016 of the *G-7 Fundamental Elements of Cybersecurity for the Financial Sector* (*"G7FE"*).

These efforts include steps to ensure strong cyber resilience measures are assessed and evaluated, as highlighted by the *G-7 Fundamental Elements for Effective Assessment of Cybersecurity in the Financial Sector* (*"G7FE-Assessment"*), published in 2017. The G7FE-Assessment included components to consider and embed when developing cyber resilience assessment frameworks.

The *G-7 Fundamental Elements for Threat-Led Penetration Testing (G7FE-TLPT)* provide entities with a guide for the assessment of their resilience against malicious cyber incidents through simulation and a guide for authorities considering the use of Threat-Led Penetration Testing (TLPT) within their jurisdictions. These fundamental elements are intended to complement a wider suite of cyber resilience assessment tools and techniques, and are not meant to be considered as a singular approach.

The core objectives of the *G7FE-TLPT* are to enhance and assess the cyber resilience of entities and the financial sector more generally, by:

- Providing core elements of and approaches for the conduct of TLPT across G-7 jurisdictions. The G7FE-TLPT aim to facilitate greater compatibility among TLPT approaches, whilst also encouraging flexibility and local tailoring based on the unique markets and regulations within each jurisdiction;
- Providing a guide to authorities considering the use of TLPT within their jurisdiction;
- Providing a guide to entities with respect to conducting their own TLPT assessments; and
- Supporting cross-authority interaction and cross-jurisdictional TLPT for multinational entities, facilitating mutual acceptance of test results.

The *G7FE-TLPT* seek to drive greater compatibility among TLPT approaches and do not invalidate existing frameworks or prevent their continuous adaptations to the evolving threat landscape.

What is TLPT?

TLPT[1] is ***a controlled attempt to compromise the cyber resilience of an entity by simulating the tactics, techniques and procedures of real-life threat actors. It is based on targeted threat intelligence and focuses on an entity's people, processes and technology, with minimal foreknowledge and impact on operations***.

What is the purpose of a TLPT?

The purpose of TLPT is to assess and provide insights on entities' resilience capabilities against a real world simulated cyber incident. TLPT should be conducted within a set scope and incorporate a risk management process to ensure a controlled test that minimizes risk to entities.

Who is G7FE-TLPT for?

The *G7FE-TLPT* are designed to provide a guide to: (i) authorities considering the use of TLPT for the design, implementation and management of TLPT in their respective jurisdictions; (ii) entities undertaking TLPT; (iii) organizations providing cyber threat intelligence services ('threat intelligence providers'); (iv) organizations providing penetration testing services ('penetration testing providers'); and (v) accreditation and certification providers[2].

The application of the *G7FE-TLPT* is non-binding. However, authorities could incorporate TLPT in their assessments of certain entities' cyber resilience by considering, among others, the following factors:

- The extent to which cyber resilience is a priority from the financial stability and market integrity perspective;
- The significance of some entities that provide critical functions and services across the financial sector; and
- The (un)availability of other risk assessment tools and techniques for testing cyber resilience.

Authorities may also consider proportionality to accommodate for the type, size, complexity, sophistication and risk profile of the targeted entities.

In cases of multinational entities, authorities across different jurisdictions should plan, collaborate and coordinate such tests to achieve the optimal outcome in terms of timing, scoping and implementation.

Effective TLPT involves strong multi-stakeholder engagement throughout the assessment process. For entities involved in cross-jurisdictional assessments, prior to the TLPT engagement, the entities should define the list of participating authorities as appropriate. This aims to support cross-jurisdictional assessments, promote discussions with respect to mutual acceptance of TLPT results of multinational entities across jurisdictions and develop protocols for the sharing of deliverables from the TLPT assessment.

[1] In some jurisdictions this may be referred to Ethical Red Teaming.

[2] The accreditation and certification provider validates the vendors' baseline level of proficiency to provide threat intelligence and penetration testing services.

Information Sharing and Data Protection
The entity is responsible for conducting a TLPT assessment and sharing deliverables in accordance with the requirements of all relevant authorities. Such authorities may wish to collaborate on information sharing, where appropriate, and consistent with data protection and cross-jurisdictional information sharing norms.

Effective controls should be in place to protect details of all information related to TLPT activities. Controls should reflect the sensitivity of the information. Information should be distributed on a need-to-know basis.

TLPT Fundamental Elements
To meet the overall goals of TLPT, the *G7FE-TLPT* set out six fundamental elements for authorities and entities to consider when developing and conducting TLPT, providing clarity on the responsibilities of the different stakeholders at each phase. In general TLPT comprises the following phases: Scoping and Risk Management, Threat Intelligence, Penetration Testing and Closure.

Element 1: Scoping and Risk Management
There are inherent potential risks associated with TLPT for all stakeholders. In line with the potential risk, the *G7FE-TLPT* place high priority on clearly defining the scope of the test and applying effective risk management controls throughout the entirety of the assessment.

Roles and Responsibilities
The White Team[3] is responsible for ensuring appropriate risk management controls are in place and getting agreement on the scope of the test with the relevant stakeholders. As the test would be conducted without the foreknowledge of the Blue Team[4] to enable the Red Team[5] to effectively assess the entity's resilience capabilities, the White Team is encouraged to perform the project management role throughout the assessment process including the Scoping and Risk Management phase.

Scope
Primarily, the test scope should be based on an assessment of the critical functions and services of the entity, which in turn will inform decisions on the test's duration and confirm inclusions or exclusions of parameters. The entity should identify the underlying people, processes and technology supporting those critical functions and services, including third party providers (such as IT service providers and supply chain relationships). If the test requires the inclusion of third party providers within the scope, it is the responsibility of the entity to liaise and ensure the participation of the third party provider.

[3] The White Team is the group responsible for coordinating an engagement between a Red Team of simulated threat actors and a Blue Team of actual defenders of their entity's use of information systems. During a test, the White Team enforces the rules of the exercise, observes the exercise, resolves any issues that may arise, receives all requests for information or questions and ensures that the test is executed in the intended manner.
[4] The Blue Team is the group responsible for defending an entity's use of information systems by maintaining its security posture against a group of simulated threat actors (i.e. the Red Team).
[5] The Red Team is the group of testers, authorised and organised to emulate a potential actions of a threat actor or exploitation capabilities against an entity's security posture.

The entity should understand any scoping requirements of the authorities in relevant jurisdictions and is encouraged to analyze their respective requirements. This is particularly important if the entity wishes to use the results to satisfy any TLPT requirements of authorities from these jurisdictions. In such cases, the entity should incorporate and liaise at the initial scoping phase with all relevant authorities, who may provide guidance to the entity on the test scope.

During the lifecycle of a test, the scope and duration may evolve as a result of interactions between threat intelligence and penetration testing providers, based on the results of their work. There should be agreement by the relevant stakeholders (the entity, threat intelligence and penetration testing providers, authorities, etc.) on the modifications to the scope with regard to the authority's requirements.

Risk Management

Entities, in consultations with their relevant stakeholders, should apply effective risk management controls to reduce the risk of any potential impact to entity data, damage to entity assets and disruption to critical services and/or operations at the entity or in the financial sector. As part of risk management, the White Team may halt the test at any point, if it considers that continued testing poses an unacceptable risk to the entity.

While communication within the entity should be kept to a minimum to protect the integrity of the test, the entity should ensure appropriate risk management controls are communicated and understood by all relevant stakeholders.

Findings Classification

During the Scoping Phase, stakeholders, including the penetration testing providers, should reach agreement on the classification schema for vulnerabilities discovered during testing, as well as on objectives that demonstrate successful compromise of the entity. The classification schema aims to show criticality and priority of discovered vulnerabilities in line with the entity's risk management framework.

The scoping deliverable should be provided to the threat intelligence provider to help develop intelligence-based scenarios for testing critical services.

Element 2: Resourcing

The entity is responsible for procuring threat intelligence and penetration testing providers. Due to the sensitive nature of TLPT, entities should carefully select the threat intelligence and penetration testing providers, based on factors such as level of expertise, ethical code of conduct and adequate levels of assurance (e.g., indemnity insurance). Accreditation and certification can be a method of validating the expertise of such providers.

While external threat intelligence and penetration testing providers generally offer an independent perspective, their use may be subject to jurisdictional requirements. Entities should confirm their approach meets the requirements of target jurisdictions at the scoping phase of the process. For example, some jurisdictions may mandate the use of external threat intelligence and penetration testing providers and validation of expertise by accreditation and certification providers.

Element 3: Threat Intelligence

Threat Intelligence is a core phase of the overall TLPT process. Threat intelligence providers use threat intelligence and reconnaissance focused on the entity to create credible threat profiles which, mimicking real-life cyber threat actors, are critical to the scoping of testing activities. The threat profiles contain cyber threat scenarios which help the Red Team develop test plans, used during the Penetration Testing phase.

Roles and Responsibilities

The threat intelligence provider is typically responsible for: (i) producing threat intelligence deliverables, aligned to the scope of test, and in accordance with direction provided by the entity; (ii) justifying the relevance of the threat intelligence deliverables; (iii) disseminating threat intelligence deliverables to the White Team; and (iv) providing support, as required, to the Red Team. This includes helping to develop the cyber threat scenarios, as well as fulfilling any new intelligence needs that occur as the Penetration Testing phase progresses.

The entity should provide: (i) direction to the threat intelligence provider regarding functions or systems in scope; (ii) additional background information to assist the threat intelligence provider in the timely and effective development of the threat profiles; and (iii) threat intelligence deliverables to the penetration testing provider, appropriate stakeholders, and authorities as needed.

Threat Intelligence Competencies

Effective threat intelligence providers typically demonstrate the following minimum capabilities:

- Ability to profile cyber threat actors relevant to the entity, sector and geographical region;
- Ability to produce cyber threat scenarios, replicating the methodology of chosen threat actors;
- Utilization of different methodologies and multiple sources and types of intelligence, such as Open Source Intelligence (OSINT) and industry related Indicators of Compromise (IoCs), to fully develop an accurate and up-to-date picture of an entity's vulnerable attack surfaces, focusing on people, processes and technology; and
- Multi-language intelligence collection ability.

Threat Intelligence Deliverables

For each TLPT engagement the threat intelligence provider should produce deliverables that contain the following types of information:

- Threat Intelligence Report (TIR) – The TIR should contain profiles of cyber threat actors who represent a credible threat to the entity. Where no specific reporting relating to the entity is available, actors may be selected based on previous known activity within relevant sectors or regions. Each threat actor profile should contain a cyber threat scenario that best highlights the methodology and tools utilized by the threat actor. Cyber threat scenarios should be detailed enough to provide penetration testing providers with all relevant approaches and information required to formulate effective test plans.
- Targeting Report (TR) – The TR should provide a profile of the entity that highlights vulnerable or exposed attack surfaces relevant to people, processes and technology, in accordance with the scope. The report should seek to provide the penetration testing provider with potential threat vectors into the target entity.

Prior to inclusion within the Penetration Test Plan, a coordinated approach should be developed that allows the stakeholders to challenge the threat intelligence deliverables, and to map the agreed-upon cyber threat scenarios to in-scope systems. This coordination, generally facilitated by the entity, allows the Red Team to develop a more focused Penetration Test Plan in line with the primary objectives of the test.

Throughout this process, and during the Penetration Testing phase, the threat intelligence provider should continue to offer their expertise, as and when required. In cases of entities offering services in various jurisdictions, the different stakeholders should take due consideration of sharing the deliverables across jurisdictions, given the sensitivity and confidentiality of the information.

Element 4: Penetration Testing

Following completion of the Threat Intelligence phase, the Red Team should plan and execute a test of the target systems and services, as defined in the scope. It is recommended that based on the scope, sufficient time be allocated to the Penetration Testing phase to allow the Red Team to conduct a realistic test in which the cyber threat scenarios are executed.

Roles and Responsibilities

The Red Team is typically responsible for the following: (i) producing a Penetration Test Plan, aligned to the scope and risk management processes, which clearly sets out the scenarios to be followed during the test; (ii) conducting the test in accordance with the cyber threat scenarios generated from the output of the threat intelligence provider; and (iii) drafting and issuing the final Penetration Test Report to the entity.

The White Team is responsible for: (i) coordinating and facilitating test activities; (ii) maintaining continuous dialogue with the Red Team and providing additional support where necessary; (iii) overseeing and monitoring the Blue Team; and (iv) applying effective risk management controls (including halting the test at any point, if deemed necessary).

The relevant authorities may observe the test alongside the White Team.

Test Methodology, Approach and Deliverables

The entity should conduct a TLPT assessment in accordance with the requirements of the relevant authorities from whom they wish to seek acceptance of the test.

The Red Team should utilize the threat intelligence deliverables to develop a targeted Penetration Test Plan. The entity should ensure that the Red Team is afforded sufficient time to appropriately conduct the test.

In accordance with the risk management controls, the White Team should monitor the execution of the test throughout, to ensure risks to target system(s) are minimized.

The entity should have an understanding of testing requirements for production and non-production environments, as these may be subject to mandatory requirements in some jurisdictions.

On conclusion of the test, the Red Team should produce a Penetration Test Report. This report should include details of the approach taken for testing as well as the findings and observations from the test. It should evaluate the risks and existing controls and, where necessary, provide advice regarding areas for improvement.

Element 5: Closure and Remediation

Following completion of the Penetration Testing phase, the TLPT moves into the Closure phase, which aims to allow all relevant stakeholders to analyze and respond to the outcome of the test and make improvements to further enhance the cyber resilience of the tested entity.

The penetration testing provider is typically responsible for supporting any post-test workshops including the presentation of findings to the entity.

The entity is responsible for: (i) distributing the findings to the appropriate stakeholders using agreed upon secure delivery means; (ii) arranging post-test workshops with the relevant stakeholders to discuss the findings and identify potential mitigation solutions; and (iii) producing and executing upon a full remediation plan.

The relevant authority is responsible for engaging with the entity and agreeing on the remediation plan; and following up on the execution of the remediation plan as part of its normal engagement with the entity.

Element 6: Thematic data

One of the core objectives of the *G7FE-TLPT* is to contribute to the improvement of the cyber resilience of entities and the financial sector more generally. An important means of achieving this is the production and sharing of thematic data amongst authorities and entities.

Thematic data should identify common sector findings and vulnerabilities. All thematic results must prevent identification of individual entities. Jurisdictions have the discretion of using their own recognized frameworks as the base for creating post-TLPT thematics and the production of thematic data relating to TLPT engagements is the responsibility of the relevant authorities. Authorities may consider a number of approaches to information sharing, where appropriate and consistent with data protection and cross-jurisdictional information sharing norms.