Varying shades of red: how red team testing frameworks can enhance the cyber resilience of financial institutions[1]

Executive summary

The cyber resilience[2] of financial institutions is one of the most critical concerns among financial sector authorities. As financial institutions become more digitalised and the sophistication of threat actors increases, financial institutions are becoming more exposed to cyber threats. Senior policymakers have warned that such threats could disrupt financial services and undermine security and confidence. From a supervisory perspective, consideration should be given to the potential of failure of a financial institution due to cyber weaknesses. Moreover, the possible contagion from such an event across the financial sector could give rise to systemic implications, and thus threaten financial stability.

Financial institutions and authorities are taking steps to strengthen the cyber resilience of firms. Financial institutions can use existing standards as a basis for strengthening their cyber resilience capabilities, and a range of testing activities to validate those capabilities. While each type of test has its intended objective, there is recognition of the importance of threat intelligence-led simulation of real-life cyber attacks through red team tests. Red team tests are useful to identify potential weaknesses in financial institutions' cyber protection, detection and response capabilities in order to establish an effective remediation plan.

This paper aims to facilitate deeper understanding by financial sector authorities on different existing approaches that authorities have pursued in establishing red team testing frameworks. The paper is based on information provided by eight financial authorities and selected private sector players. It describes key components of a red team testing framework, compares existing frameworks, outlines the benefits and challenges of such frameworks, and highlights potential cross-border issues relating to red team testing.

In general, a red team test can be divided into four phases: reconnaissance; getting into the institution; getting through its systems; and getting out with the captured "flags" as defined in the scenarios. Red teams can use either a methodology with a clear sequence of events in a cyber attack life cycle, or one that focuses on techniques from the different tactics deployed by threat actors and jumps from one point in the attack life cycle to another depending on the situation. In terms of scope, a red team test typically covers the entire financial institution involving different teams, potentially including external threat intelligence[3] and test providers.[4] The test is conducted without the knowledge of those responsible for protecting the institutions from cyber attacks.

Most of the surveyed jurisdictions have established red team testing frameworks with a number of common elements. The frameworks generally involve the following steps: defining the scope and risk management controls for the test; procuring threat intelligence and red team providers; gathering

[1] Jermy Prenio (jermy.prenio@bis.org) and Jeffery Yong (jeffery.yong@bis.org), Bank for International Settlements; Raymond Kleijmeer (r.kleijmeer@dnb.nl), the Netherlands Bank. The authors are grateful to contacts at the financial authorities covered in this paper and to Juan Carlos Crisanto, Matthew Hayduk, Rastko Vrbaski and David Whyte for helpful comments. Bettina Müller and Giada Tossi provided valuable administrative support with the paper.

[2] The Financial Stability Board Cyber Lexicon defines cyber resilience as the ability of an organisation to continue to carry out its mission by anticipating and adapting to cyber threats and other relevant changes in the environment and by withstanding, containing and rapidly recovering from cyber incidents.

[3] Threat intelligence refers to information on cyber threats facing an industry or a specific institution (eg specific threat actors likely to target the institution and the likely tactics, techniques and procedures that they will utilise). In the red team testing context, such information may be provided by external private sector parties.

[4] These are private sector institutions whose service consists in providing the red teams with which to conduct red team tests.

threat intelligence; conducting the actual test; analysing the test outcomes; putting in place a remediation plan; and sharing the lessons learned with stakeholders.The frameworks apply typically to large or critical financial institutions, but authorities may have discretion to include other financial institutions. The frameworks, however, differ in terms of whether threat intelligence and red team test providers must be external to the financial institution, accredited and formally assessed.

An effective red team test is characterised by both firms and authorities being open about the results, learning from the weaknesses exposed and taking appropriate remedial actions. Unlike other risk assessment exercises, a successful red team test is not determined by whether a firm "passes" or "fails" the test. To truly benefit from red team testing, focusing on implementation of remediation measures after the test provides more value than just focusing on the test outcomes as evidence of weaknesses in the institution's cyber practices.

In the red team testing frameworks covered, financial authorities have different levels of involvement in the tests. In some cases, authorities are more involved and typically manage the conduct of the tests (ie oversee and guide the process of the test from start to finish, but do not take over responsibility of the test from the institution being tested). In other cases, authorities are less involved and instead focus their cyber resources on supervisory activities such as assessing the adequacy of financial institutions' cyber resilience, including ensuring that remediation measures identified during the red team tests are implemented in practice.

Sound technical and business expertise on the part of those involved in red team tests within firms, external threat intelligence and test providers as well as authorities is particularly important to ensure high-quality tests. Some authorities require external providers to be accredited or qualified so as to define a baseline of requirements for testers. In certain jurisdictions, the authorities do not require formal accreditation or qualification for several reasons, particularly scarcity of technical experts. Such flexibility is warranted to allow expertise to be cultivated while enabling firms to carry out the tests.

Establishing proper controls is also necessary to ensure the quality of the tests and to mitigate the risks. To help achieve high-quality tests, the existing red team testing frameworks describe expectations on procedural arrangements that should be put in place for the tests. These include expectations in terms of the scoping of the test, the selection of threat intelligence and red team providers, the formation of different teams and outlining their responsibilities. These procedural arrangements help in establishing a trusted environment among the different parties involved in the red team testing. In addition, these arrangements also enhance proper controls to mitigate risks associated with red team tests (eg risks to production systems and to sensitive information).

From a cross-border perspective, certain authorities may be prepared to recognise red team testing conducted under another jurisdiction's framework if certain conditions are met. Moreover, coordinated cross-border red team testing by financial institutions may be necessary to avoid jurisdictional blindspots and minimise unnecessary duplication of efforts by firms and authorities. This is especially useful for financial institutions with centrally managed infrastructures operating in jurisdictions with compatible frameworks. However, technical, operational and legal challenges surrounding such exercises are not easy to overcome currently.

Going forward, financial authorites may wish to clarify how red team tests fit within their strategy to improve the cyber resilience of financial institutions. Given that red team testing approaches are still evolving, it is important that authorities continue to assess the effectiveness of their frameworks and use the lessons learned from each test to improve the overall cyber resilience of the financial sector.