# 8. Three typical cyber-attacks: how TIBER-BE approaches threat-led red teaming scenarios

Jean-Louis Buchholz and Samuel Goret

Given the constantly evolving nature of cyber threats, the financial sector faces unprecedented challenges which require innovative testing methodologies. TIBER-EU (Threat Intelligence-Based Ethical Red Teaming for financial institutions in Europe) stands at the forefront, offering a proactive approach to cybersecurity testing. As cyber threats become increasingly sophisticated, financial institutions must prioritise their defence strategies. This article delves into the relevance of TIBER-EU, its focus on critical threats and representative three-scenario approach designed to strengthen the capabilities of institutions to potential cyber adversaries. TIBER-BE, the Belgian implementation of the framework endorsed by the European Central Bank, leverages ethical red teaming to execute realistic cyber threats on live production systems, within legal and ethical boundaries as well as budget and time constraints. Faced with an intricate landscape of threats, TIBER-BE helps institutions pre-emptively address vulnerabilities by employing a customised threat assessment and targeted testing methodology.

Before turning to the three scenarios, it is important to acknowledge the prevailing threats in the financial sector. Advanced persistent threats (APTs) and phishing campaigns are omnipresent. TIBER-BE recognises the need to simulate these threats comprehensively, ensuring financial institutions are prepared to deal with complex modern cyber risks. Insider threat scenarios, although less likely, provide a perfect middle ground to cover tactics and techniques used by a wider variety of malicious actors, without the risk of the test being detected in the early stages of the attack.

### *The three-scenario approach*

TIBER-BE's three-scenario approach orchestrates a strategic progression, starting from sophisticated internal threats and ending with external phishing attacks, an initial access tactic more likely to trigger detection. This reverse order aims to maximise learning by prioritising responses to subtler threats. It should be noted that this approach is customised to the targeted threat intelligence level and specificities of the institution being tested.

### *Scenario 1: an advanced persistent threat in the form of a "living off the land" attack*

Objective: Detect and respond to an advanced persistent threat (APT) deeply embedded in the network. The purpose of the attack could be pre-positioning for espionage, disruption or further compromise of the supply chain.

1. Initial access: simulate a sophisticated attack with unauthorised access to specific infrastructure.
2. Persistence and evasion: establish persistence mechanisms to maintain long-term access and employ techniques such as fileless malware and anti-forensic measures to evade detection.

3. Lateral movement: mimic lateral movement within the network, leveraging legitimate tools to avoid suspicion and opting for "living off the land" tactics and misconfigurations for malicious activities.
4. Data exfiltration: simulate the extraction of sensitive information without triggering alarms and evaluate the institution's ability to detect and respond to data exfiltration attempts.
5. Data/system wipe: introduce or emulate a (controlled) ransomware or data wiping to assess the institution's preparedness and response capabilities to a critical incident.
6. Supply chain intrusion and third-party dependency: simulate the infiltration of the financial institution's supply chain to assess vulnerabilities in external connections and evaluate the impact of an assumed breach on interconnected third-party systems within the supply chain of the financial sector.
7. Response evaluation: assess the speed and effectiveness of the financial institution's response to the breach scenario with a focus on minimising the dwell time of the attacker within the network.

### *Scenario 2: insider threat*

Objective: Identify and mitigate the risks associated with an insider threat with limited hacking capability but legitimate access and insider business or ICT knowledge.

1. Simulated insider access: emulate an insider with restricted access attempting unauthorised actions within the system.
2. Persistence and defence evasion: perform subtle data manipulations to test the institution's ability to detect unauthorised changes and evaluate the effectiveness of the anomaly detection mechanisms. Persistence is trivial given that the threat is an employee or a contractor with legitimate access to the systems.
3. Lateral movement: navigate applications and file sharing to look for misconfigured authorisations, unprotected sensitive data or applications that can benefit from an insider perspective.
4. Covert communication: mimic discreet communication channels to avoid detection and assess the institution's capabilities to detect unusual communication patterns.
5. Incident response: gauge the institution's incident response readiness and evaluate communication and collaboration among response teams.

### *Scenario 3: phishing and external perimeter attack*

Objective: Assess the institution's resilience to a typical external attack, focusing specifically on phishing and attacks targeted at externally exposed assets.

1. Phishing simulation: launch (spear-)phishing campaigns against carefully selected employees to evaluate susceptibility and measure the effectiveness of email filtering and employee awareness training.
2. Malware deployment: simulate malware delivery through phishing vectors and evaluate the institution's static and behavioural endpoint protection and malware detection capabilities.
3. Credential harvesting: emulate credential harvesting techniques to assess the institution's defences against unauthorised access and test the effectiveness of multi-factor authentication.
4. Post-phishing activities: assess the institution's ability to detect and respond to activities following successful phishing attacks and evaluate the speed of isolating compromised accounts and systems.

### *Conclusion*

TIBER-BE's evolving three-scenario approach, enhanced by considerations related to supply chains, enables financial institutions to assess their capabilities in the current cyber threat landscape. By synthesising realistic threat simulations, institutions can develop an effective remediation plan to proactively enhance their cybersecurity resilience and fortify their defences against the emerging challenges of the digital era.

# 9. Shortening the settlement cycle in European securities markets

Steven Van Cauwenberge

To reduce unnecessary risks and improve efficiency in capital markets, regulators are increasingly focusing on shortening the settlement cycle for securities trades.

With the adoption of the CSD Regulation in 2014, the EU moved from standard settlement of securities trades within three business days from the trade date (T+3) to two business days (T+2), with the US following suit in 2017. The US has now shortened its settlement cycle further and, since the end of May 2024, ensures settlement by the next business day (T+1). The EU is considering doing likewise.

### *US move to T+1 settlement at the end of May 2024*

In February 2023, the US securities regulator (the Securities and Exchange Commission or SEC) introduced rules[1] to move from securities settlement for most broker-dealer trades from T+2 to T+1 by 28 May 2024. The SEC rules apply unless participants expressly agree otherwise. They cover all securities trades with a limited number of exceptions including, for example, municipal and government securities (albeit formally, as US Treasuries are already settled on a T+1-basis), commercial paper and security-based swaps. Derivatives trades are also out of scope, including when linked to money market trades for hedging purposes.

The final stage of a trade conducted on a stock exchange or between counterparties (over-the-counter)[2] is settlement, a process by which securities are exchanged for cash. To allow T+1 settlement, changes are required at both the trade and settlement stages.

Broker-dealers will need to implement policies or enter into written agreements to ensure that trade allocations, confirmations and affirmations with their institutional customers are completed as soon as technologically practicable and in any case no later than the end of the trade day ("same-day affirmation").[3]

After trading, buy and sell instructions must be matched to capture the trade before settlement. Central matching services providers[4] – such as the CSD DTCC in the US and both EU international CSDs – will have to report to the US supervisor on their straight-through processing, so as to allow the timely processing of trades.

1 Available at https://www.sec.gov/files/rules/final/2023/34-96930.pdf.

2 The post-trade settlement process could also include a clearing stage whereby a central counterparty interposes itself between the buyer and the seller.

3 Allocation is the process of assigning executed trades to different accounts or portfolios, ensuring that each account receives the appropriate number of securities. Confirmation is the process whereby the terms of a trade are verified – and confirmed – between the market participants directly involved. Affirmation refers to the same process but between a market participant (e.g. a broker) and their professional customer (e.g. an institutional investor).

4 Central matching service providers help facilitate the processing of institutional trades between broker-dealers and their institutional customers.

Generally speaking, T+1 settlement will not substantially impact settlement by CSDs, given that they already can and do settle the next day (T+1) or even intraday (T+0) in most cases. However, it will clearly impact the operations of market participants (i.e. at settlement level), of CSD participants and of their underlying clients.

For dual listings, trading venues in the EU can continue to use a T+2 settlement cycle for EU trading venues, in line with the CSD Regulation. Nonetheless, dual listing will lead to demands to coordinate corporate events, as their occurrence depends on the settlement period used.

### *Benefits of moving to a shorter settlement cycle*

A shortening of the settlement cycle implies a reduction in counterparty credit risk and related capital costs over the settlement period. When conducting a trade, the buyer has a position in the purchased security from the time the trade is concluded (at day T) notwithstanding later delivery of the security at settlement. Upon delivery, the market price of the security may be higher, and the buyer thus bears, over the settlement cycle, counterparty risk for the cost of the security. All things being equal, the market price of a security will be less volatile over a period of one day than two. To cover this risk, the buyer will need – based on standard distribution assumptions – around 30 %[1] less capital or margin in a T+1 scenario compared with a T+2 scenario.

Market makers need to have cash and securities on hand in order to provide their services. When they do not carry the positions as inventory, they can borrow the securities or cash needed using securities as collateral, although this also requires capital or a margin. The funding possibilities and conditions of the market maker will therefore impact the market liquidity of the securities.

The (costs of the) counterparty and liquidity risks of the market maker will be reflected in the bid-ask spreads they offer. A shorter settlement cycle can be expected to reduce the capital or margin needs for intermediaries and thus diminish bid-ask spreads. Furthermore, a shorter cycle generally reduces the market value of the outstanding transactions trapped and awaiting settlement at any time.

Assuming timely settlement, T+1 settlement will allow the holders of securities to realise cash in a shorter timeframe. This can be especially advantageous in a stressed market in which participants are seeking cash.

From an operational point of view, T+1 settlement will require the industry to use straight-through processing and thus lower operational risk as manual procedures are replaced.

These advantages should be considered against the possible drawbacks and costs.

### *Costs of moving to a shorter settlement cycle*

While it is argued above that a shorter settlement cycle will increase liquidity, the opposite view can be held. A shorter cycle limits the time market makers have to find counterparties. Market makers may incur additional costs to borrow securities or cash which could lead to reduced market liquidity. Also, a broker or CCP may not (fully) reduce the collateral requirement for its counterparties, as it may deem that the period needed to replace a failed trade could take longer than one day.

Also, from an operational point of view, there will be less time to settle trades under a T+1 regime. The industry has indicated that – given customary working hours – the effective window to process a trade after its conclusion

1 This is assuming price changes in the market are normally distributed. Under this statistical assumption, price movements correlate with the length of the settlement period on a "square root" basis, meaning, all other things being equal, reducing the settlement period from two days to one will not halve volatility but reduce it by 30 % (roughly the ratio of the square roots of 1 and 2). This rule of thumb is referred to, for example, in a January 2024 speech on T+1 settlement given by the SEC chair before the EU Commission, available at https://www.sec.gov/news/speech/gensler-speech-prepared-remarks-european-commission-012524.

would diminish by 80 %.[1] To settle on day T+1 requires same-day trade allocation and confirmation, which is challenging for market participants. Operating in a different time zone exacerbates these requirements. Further automation efforts will be needed. Investing in straight-through processing, across a broad range of functions, implies costs. CSDs could be asked to extend their opening hours to allow later cut-off times to accept settlement instructions. Market participants may even consider changing the location of their staff or, alternatively, "operational" outsourcing to local custodians that offer broader services.

A shorter settlement cycle increases the risk of settlement failure. Heightened fail rates – for example, an estimated 15 %-35 % increase in the current fail rates for the US market[2] – are expected to be seen at least temporarily after the transition to a shorter cycle.

Moreover, alignment issues will arise where settlement cycles diverge. The liquidity implications of these may depend on the instrument. For funds, for example, the underlying securities may trade with a diverging settlement cycle, leading to the need for improved cash liquidity and/or securities inventory management.

In addition, a given security could settle on either day T+1 or day T+2 depending on where it trades. This is the case for Euromarket securities listed on both a UK and an EU market. Dealers may reflect their funding costs in their trading prices, resulting in possible differences in bid-ask spreads across trading venues[3].

Finally, when the need arises to source foreign currency liquidity in FX markets that continue to operate on day T+2, risks and costs may increase. There is no corresponding initiative for the FX spot market to shift to T+1,[4] which implies obstacles for investors funding security transactions in a non-domestic currency. In addition, CLS deadlines could be missed, potentially leading to the increased use of bilateral FX settlement.[5]

### *EU initiatives regarding a move to T+1 settlement*

In general, the settlement cycle is determined by the location of the trading venue, not the place of settlement. The securities falling within the scope of an eventual EU decision to move to T+1 settlement are expected to be determined by the scope of the current T+2 requirement. Today, Article 5(2) CSDR sets T+2 as a maximum settlement cycle for securities trades executed on an EU trading venue. Trading parties can – at least in principle – voluntarily agree to a shorter period. Also, counterparties that trade bilaterally can in theory agree on any settlement cycle they wish, including a longer one. The assumption is however that market participants will usually follow the standard set for transactions in the trading venue.

Under the coordination of the Association for Financial Markets in Europe (AFME), a cross-industry working group has been established to study both the impact on EU markets of the US's move to T+1 settlement and the potential migration to T+1 in the EU. The group represents 15 associations of investment managers, trading venues, CCPs, CSDs, broker-dealers, custodians and product-specific experts.

Markets are not expected to move to T+1 settlement on a voluntary basis. Regulatory intervention will thus be required. The CSD Refit Regulation mandated ESMA to produce a report on the costs and benefits of a shortened settlement cycle in the EU. As a first step in this process, ESMA launched a market consultation ("call

1 See the report of the Association for Financial Markets in Europe (AFME) published in September 2022, available at https://www.afme.eu/Portals/0/DispatchFeaturedImages/AFME_Tplus1Settlement_2022_04.pdf.

2 As referred to in the ESMA feedback statement on its "Call for evidence on shortening the settlement cycle". Fail estimates are discussed on page 27, nos. 99-105.

3 This point is discussed in the report of the UK's Accelerated Settlement Taskforce.

4 Although, notably, the SEC chairman called for considering this in the abovementioned speech.

5 Continuous Linked Settlement (CLS) is a US-based international payment system which was launched in September 2002 for the settlement of foreign currency exchange. Settlements in CLS occur payment-versus-payment and thus avoid principal risk in the event of counterparty default. A CLS press release from early April 2024 deemed the problem to be minimal and in need of further assessment after the US transition to T+1 securities settlement, prior to a decision being taken on possible changes to CLS settlement timelines. See https://www.cls-group.com/news/update-on-the-potential-change-to-clssettlement-timelines-following-the-move-to-tplus1-securities-settlement/.

for evidence") on 5 October 2023. ESMA plans to publish its final report to the Commission at the end of 2024. Quantifying the costs and benefits of a shorter settlement cycle appears challenging.

An EU move to a shorter settlement cycle must be judged on its own merits. The EU market is different than the US or other markets due to a far more fragmented infrastructure, making cross-border settlement, in particular, more complex.

To the extent banks operate globally and markets are interconnected, a worldwide harmonisation of settlement periods could be pertinent. However, the EU does not necessarily need to move at the same time as other jurisdictions. Canada and Mexico will move to T+1 settlement in lockstep with the US, as their markets are clearly interconnected. As the proportion of dual US-EU listings or of EU trades in the US market seems relatively modest, it does not appear absolutely necessary for the EU to move to T+1 settlement at the same time. EU market participants indicate that the UK market's potential move to T+1 settlement would be more relevant to them, as the EU and UK markets are more closely intertwined.

The UK established an Accelerated Settlement Taskforce to analyse this issue, which published a report at the end of March 2024.[1] The report noted a broad consensus to move. It elaborates on the hurdles and requests the establishment of a technical group to further consider the specific details of a move. It envisages a two-step approach for the transition. The move to T+1 settlement, which is planned to take place before the end of 2027, would be preceded by the introduction of a requirement, in mid-2025, for operational processes as well as allocations, confirmations and trade level matching, to take place on the trade date. Finally, the report indicates that while a move to T+0 is not appropriate at this stage, T+1 investments should already bear in mind such an evolution.

Further, the CSD Regulation imposes cash penalties for late settlement on a per transfer basis; this rule was not taken over by the UK when it formally adopted EU legislation at the national level after Brexit. A requirement to settle on day T+1 may increase settlement fails and the ensuing penalties and add to the cost of settlement in the EU.

An EU move will most likely not occur in the next few years as the industry has indicated that it needs at least two years to plan and implement such a decision. Lessons can be learned from other markets moving to T+1 settlement, such as the US. Preparing the transition and industry-wide testing of processing in T+1-mode will be key for market participants. CSDs and the T2S platform may play a role here. Supervisors of CSDs and market participants will be expected to monitor the situation.

### *Conclusion*

Following the move by the US to T+1 settlement, the EU will have to decide whether to move to a shorter settlement cycle. In January 2024, the EU commissioner responsible for financial services, financial stability and capital markets union stated that the question is not if the EU will transition to T+1 but how and when.[2] Back in 1989, the Group of Thirty – a body comprised of industry representatives and central bankers, which recommended T+3 settlement at the time – recognised that "to minimise counterparty risk and market exposure associated with securities transactions, same day settlement is the final goal".[3] Shortening the settlement cycle can bring clear benefits, improve overall efficiency, mitigate credit and liquidity risk and enhance the use of capital. But it is not without costs – at least in the short term – or certain risks that will need to be managed. In 2024, the adoption of (end-of-day) same day settlement (i.e. T+0) is still not a realistic near-term policy option as it would require a much more fundamental overhaul of the capital markets, FX/payments and securities

1 The March 2024 report of the UK's Accelerated Settlement Taskforce is available at https://www.gov.uk/government/publications/accelerated-settlement-taskforce.

2 See https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_24_422.

3 See, in this respect, Recommendation 3 in Annex C to the CPMI-IOSCO PFMI (available at https://www.bis.org/cpmi/info_pfmi.htm), derived from the 2001 Recommendations for Securities Settlement Systems which remain in effect today.

services processes. The move to a T+1 settlement cycle will require substantial system improvements, mainly by market participants rather than FMIs, to avoid increased settlement fails. Replacement cost risk may not diminish as anticipated due to a reduction in liquidity risk that is less substantial than expected. As regards overall implementation, careful planning and monitoring by the industry, regulators and supervisors will be required.

## Editorial Committee