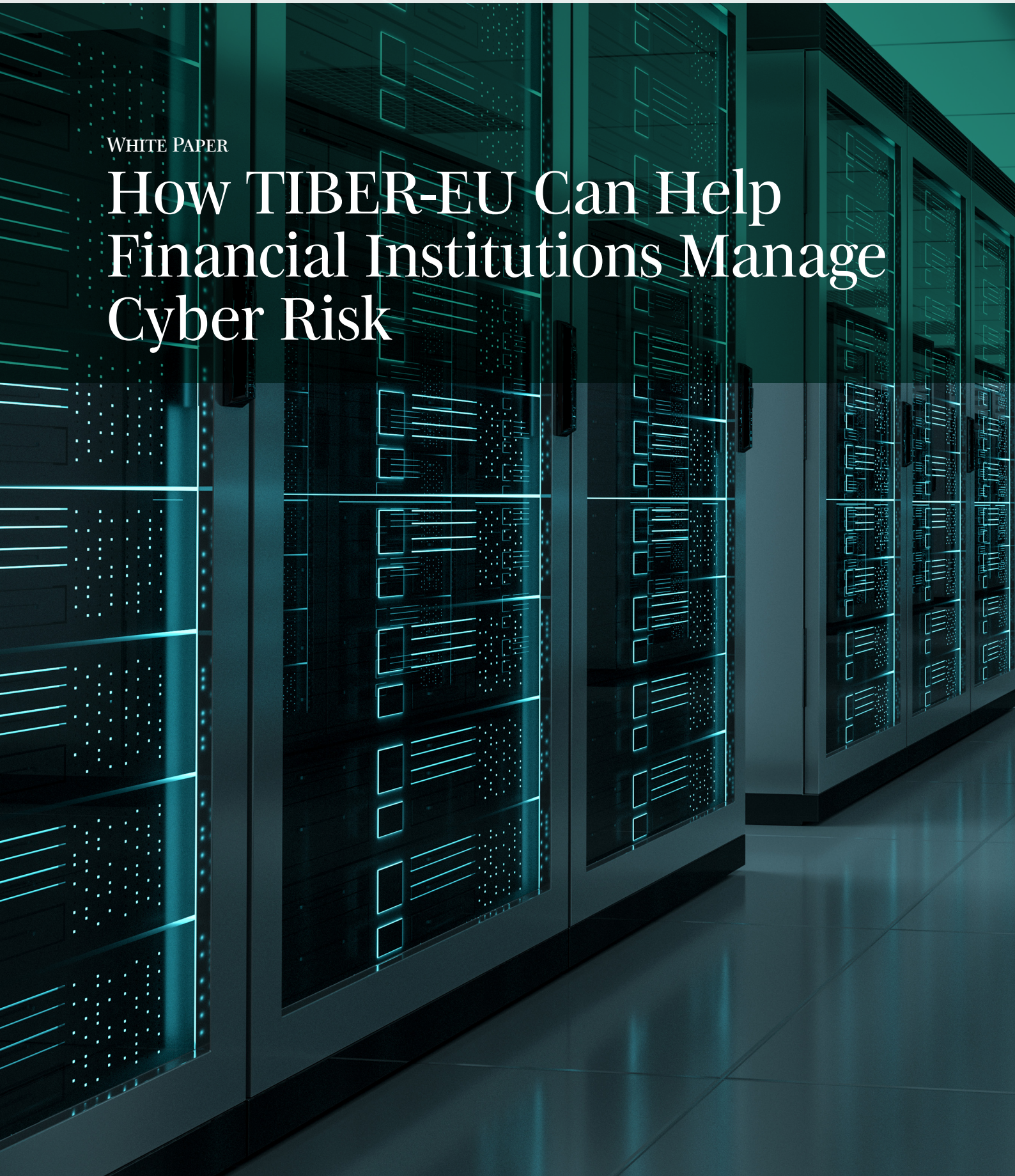
BCG

THE BOSTON CONSULTING GROUP

QuoScient



WHITE PAPER

How TIBER-EU Can Help Financial Institutions Manage Cyber Risk

The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients from the private, public, and not- for-profit sectors in all regions to identify their highest-value opportunities, address their most critical challenges, and transform their enterprises. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with offices in more than 90 cities in 50 countries. For more information, please visit bcg.com.

QuoScient is a Frankfurt based cyber-defense company. Our QuoLab social defense network and platform solves the core cyber problems of many companies: lack of security experts with enough operational experience, too many attacks and a limited budget for cybersecurity. Our mission is to make clients safer with the resources they already have. QuoLab provides immediate orientation, decision making and response capabilities, enabling teams to collaborate on investigations while ensuring data privacy requirements are met at any stage of the defense life cycle.

WHITE PAPER

How TIBER-EU Can Help Financial Institutions Manage Cyber Risk

By Jannik Leiendecker, Dirk Stegemann, Ioannis Bizimis, and Marco Riccardi

November 2018

AT A GLANCE

Every day the financial sector is subject to cyber-attacks by individuals, criminals and governments. And as digitization proliferates, the problem is becoming ever more acute. A rising number of digital touchpoints creates an expanding choice of windows through which cyber attackers can enter.

The European Central Bank in May 2018 published new guidance aimed at helping financial infrastructures and institutions create simulations of cyber-attacks that closely resemble those in the real world. Threat Intelligence-Based Ethical Red Teaming (TIBER-EU) supports European and national authorities in conducting the tests, which should be applied to investment and commercial banks, payment systems, central counterparties, exchanges and others (collectively referred to as entities). The test is designed to be based on threat intelligence specific to individual entities and to mimic the tactics, techniques and procedures of real-life threat actors.

TIBER-EU is currently advisory—national authorities and individual entities are under no compulsion to implement it. However, it is likely that supervisors will look to codify the guidelines over the coming years. Given that fact, and the rising menace of cyber-attacks, it makes sense for entities to start testing now.

Regulators are driving cyber resilience

As the threat of cyber-attacks intensifies, regulators around the world are becoming more proactive in helping entities protect themselves and their customers. The Financial Stability Board published a report in 2017 that showed its members had put in place 56 schemes of regulation and guidance targeted to cybersecurity and/or IT risk. Initiatives have included the European Banking Authority's guidelines, under the supervisory review process, for assessment of bank information and communications technology risk. The European Central Bank, meanwhile, has collaborated with national supervisors and bank chief risk officers, establishing a reporting framework and developing a strategy based on three pillars: cyber readiness of individual institutions, sector resilience, and strategic engagement between the regulator and the industry. TIBER-EU is published in that context. National authorities, meanwhile, are taking steps. The German supervisor BaFin, for example, in November 2017 published Bankaufsichtliche Anforderungen an die IT ("BAIT"), which set out regulatory requirements for financial sector IT systems. (See the BCG white paper: Diskussionspapier BAIT: Bankaufsichtliche Anforderungen an die IT)

TIBER-EU will support cyber testing

TIBER-EU was published following similar initiatives in the UK and Netherlands, and is informed by those experiences. The framework sets out guidelines to support national authorities in helping entities deliver an "intelligence-led red team test" of critical functions. "Intelligence led" means that a dedicated team works to identify tactics, techniques and procedures (TTPs) of potential threat actors likely to target the bank in question. A red team is a group of cyber security professionals who then attempt to breach the target's network.

Red teaming is distinguished from so-called penetration testing, which is an assessment of technical and configuration vulnerabilities, often in a single system or environment. Red-teaming, by comparison, assesses the full scenario of a targeted attack against an entity's critical functions and underlying systems (i.e., its people, processes and technologies). Attacks can take many forms, from injection of malware (spyware, ransomware, viruses and worms) to obtaining a job with the company to work from the inside.

Several financial entities already conduct red team testing for their own purposes. However, in many cases these have failed to offer sufficient insight into the entity's protection capabilities. A common problem is that the team is "threat-uninformed"—they don't base the test on real-world actors. Also, in using internal resources, objectivity is somewhat challenging. To avoid this kind of difficulty, TIBER-EU specifies that threat intelligence must be conducted by an independent third-party provider. In addition, the test should be overseen by a TIBER Cyber Team (TCT), set up by the local supervisor to bring together TIBER knowledge and capabilities at the national or European level. The TCT facilitates tests across the sector, and provides support and specialist knowledge to executives, referred to in the document as the "white team."

In the highly interconnected European financial system, it is likely that numerous authorities will require assurance on the cyber resilience of a single entity. To avoid overlap, TIBER-EU provides for mutual recognition of tests across jurisdictions.

The tests are required to be performed without the knowledge of the target entity's security team, called the "blue team." Only the white team should know about the test. This is to ensure it is as effective as possible in assessing how the target is able to protect its systems, and detect and respond to attacks. The process is divided into three headline phases, comprising preparation, testing, and closure, and an optional initial phase. (See Exhibit 1).

EXHIBIT 1 | TIBER EU's three headline phases

	Preparation phase	Testing phase	Closure phase
Key activities	Establish test mgmt. teams Define test scope Procure TI[1] and RT[2] providers	Create intelligence report Six steps to execute test	Provide 360-degree feedback Draft remediation plan
Responsible parties	TCT[3], tested entity, TI provider and red team	TCT, tested entity, TI provider, and red team	TCT, tested entity, blue team red team
Key deliverables	TIBER-EU project plan TIBER-EU scope specification	Target threat intelligence report Red teaming test	Test summary report Remediation plan Attestation

1. Threat Intelligence 2. Red Team 3. TIBER Cyber Team
Source: TIBER-EU Framework

INITIAL PHASE (OPTIONAL)

This comprises a generic assessment of the national financial sector threat landscape, outlining the specific roles of the entities, and identifying relevant threat actors and their TTPs. The assessment can help inform the attack scenarios performed during the test.

Preparation phase

This comprises engagement, scoping, and procurement. The entity establishes teams responsible for managing the test, sets the scope, and procures threat intelligence and red team providers. Board approval and regulatory validation are mandatory under the guidelines.

Testing phase

The testing phase is split into two stages—production of a targeted threat intelligence (TTI) report, and the test itself:

- **The TTI report stage.** The report must be prepared using methods and resources similar to those available to threat actors as they prepare for attack from outside the entity. Two steps are required:
  - **Target identification.** The threat intelligence (TI) team makes a detailed preliminary picture of the entity and its weak points from the attacker's perspective. Part of this information should be provided by the entity, based on a template provided by the ECB. This enables threat intelligence to be contextualized, and contributes to development of threat scenarios.
  - **Threat identification.** Here, the provider collects, analyzes, and disseminates intelligence about relevant threat actors, their current and prospected TTPs, and the likelihood of the entity being targeted.
- **The test stage.** The red team provider leverages the information in the TTI report to carry out a war-game attack on the live production systems, people, and processes that underpin the entity's critical functions. The test is designed to be implemented in six distinct steps:
  - **Reconnaissance.** The red team actively collects information about the target's people, technology, and environment. This step may also involve building or acquiring specific tools engagement. Reconnaissance should primarily be undertaken by the TI provider, although the RT provider also takes part during the build-up to the test.
  - **Weaponization.** Information is analyzed to produce a picture of the target and prepare attack and tools infrastructure.
  - **Delivery.** A critical active step in which the red team analyzes cyber or personnel vulnerabilities, or plants hardware trojans before breaking in.
  - **Exploitation.** Here, the red team's goal is to break in and compromise servers, apps, and networks, and to exploit target staff through social engineering tactics such as fraudulent emails. The exploitation step paves the way for the control and movement step.
  - **Control and movement.** After initial compromise, the red team attempts to move to other vulnerable or high-value systems.

– **Actions on target.** This entails gaining further access to compromised systems, and acquiring previously-agreed target information and data. The red team aims to complete the test and achieve the objectives set during the preparation stage.

Closure Phase

Closure is the final phase of the exercise, and comprises remediation planning and result sharing. It requires the red team to draft a report detailing the test experience and offering advice on areas for improvement. These may comprise technical controls, policies and procedures, education, and awareness. Finally, the entity should agree on a remediation plan in consultation with its supervisor.

Incorporating TIBER-EU into a cybersecurity target operating model

The key test of a cyber-ready operating model is the ability to reliably prevent attacks, detect intruders, implement a response, and carry out a recovery plan that includes communicating with stakeholders. (See the BCG Focus report: Banking's Cybersecurity Blind Spot—and How to Fix It). In addition, the model must inform daily operational capabilities, so that cyber risk is managed through a single strategic and operational approach. The model should incorporate cyber measures across the key elements of operations, from strategy and governance to organization, risk management, response and recovery, and culture. (See Exhibit 2).

The ECB's TIBER-EU framework contains detailed requirements for roles and responsibilities, risk management, and operational rules and procedures. With that in mind, banks and others should contemplate how they can incorporate these into their cyber target operating models.

Exhibit 2 | TIBER-EU should be incorporated in the target operating model

Source: BCG Analysis

TIBER-EU does not imply a requirement to fundamentally redesign the model. Rather, entities should enhance to reflect the new guidelines. The most relevant part relates to risk management. The general requirement under risk management is that entities should conduct regular assessments of regulatory requirements across jurisdictions and ensure that these are reflected in their own policies, procedures, and guidelines. This is specified by requirements that include risk assessments, response and recovery plans, and testing and improvement. The threat intelligence and red teaming exercises can be overlaid on the latter.

A threat intelligence and red-teaming case study

A (fictional) European bank aimed to gauge its exposure to cyber risk, and asked a threat intelligence and red teaming provider to help. The company carried out a threat landscape analysis, and identified three key threat actor groups. One was Cobalt Group, the notorious actor behind widespread attacks on banks and ATM jackpotting campaigns across Europe. The group emerged in 2016, stealing $32,000 from six ATMs in Eastern Europe, and in 2017 expanded its activities to focus on attacking financial institutions with spear-phishing schemes. The phishing involved trying to get employees to open emails and click on links or attachments that activated malware downloads.

In the next phase of the exercise, the TI team provided a threat actor profile intelligence report to its red team, detailing and assessing Cobalt's tactics, techniques, and procedures. Using this information, the team launched a simulated attack against the bank and was able to enter its systems and compromise critical security measures. Results from the attack helped the provider draft a threat assessment for the bank, detailing the likelihood of a Cobalt attack, the probable impact, and the level of risk, and offer a recommended course of action.

The bank adopted the plan and allocated budget to prioritize implementation. As part of that exercise, it developed more dedicated red-teaming capabilities, enabling it to tailor red-teaming exercises more effectively and to achieve a baseline reduction in risk

What should entities do next?

TIBER-EU is a comprehensive blueprint for using threat intelligence and red teaming to combat cyber risk. The framework is currently advisory, but may be made law in some countries over the coming years. Even without that, TIBER-EU represents best practice, and financial entities should take concerted steps to implement it. We see four steps that executive teams can take now:

Make testing a strategic priority and appoint a responsible person. The most obvious responsible person to take charge of TIBER-EU exercises is the chief information security officer (CISO). However, the board must ensure that the CISO is given the necessary budget and powers, and that there is a mechanism for reporting and remediation.

Identify key assets. Before any test, the entity must make efforts to "know itself." That means identifying its IP "crown jewels," which will provide a starting point for the threat intelligence exercise.

Select third-party vendors. Vendor selection is critical and should be based on the ECB's published guidelines. Entities must select threat intelligence and red teaming vendors, which can be separate or combined. Vendors must combine extensive knowledge of the evolving cyber landscape with the technical ability required to carry out tests based on likely threat actor strategies.

Carry out testing on a regular basis. Banks must decide how often they wish to conduct the tests. Testing should be regular, reflecting the fast-changing threat landscape.

The time is now

Financial institutions are in the cyber front line. Due to their rich data resources, financial assets, and relatively old and fragmented IT systems, they are primary targets. Regulators see significant threats to businesses, customers, and the financial system, and are rolling out policies and guidelines to help entities defend themselves. TIBER-EU is an important part of that effort, and it makes sense for the industry to engage without delay.

About the Authors

Jannik Leiendecker is a principal in the Munich office of The Boston Consulting Group. You may contact him by e-mail at leiendecker.jannik@bcg.com

Dirk Stegemann is a consultant in the Berlin office of The Boston Consulting Group. You may contact him by e-mail at stegemann.dirk@bcg.com

Ioannis Bizimis is the cofounder and COO of QuoScient. You may contact him by e-mail at ioannis.bizimis@quoscient.io

Marco Riccardi is head of Threat Intelligence at QuoScient. You may contact him by e-mail at m@quoscient.io

To find the latest BCG content and register to receive e-alerts on this topic or others, please visit bcg.com.

Follow The Boston Consulting Group on Facebook and Twitter.

11/18

BCG

THE BOSTON CONSULTING GROUP

bcg.com