Tomorrow's Affairs
Analysis of today
Assessment of tomorrow

By: Tomorrow's Affairs Staff

Cyber risk becomes a broader financial stability issue

On 7 July, the European Central Bank gave Eurozone banks until 31 October to demonstrate how they will defend themselves against cyberattacks accelerated by artificial intelligence; in other words, to prepare concrete plans to counter cyber threats that AI can accelerate, intensify or make harder to stop.

They are not being asked for a new digital transformation strategy, but for an operational defence plan: who is responsible, which vulnerabilities will be closed, in what order, by what means, and by when.

In doing so, the ECB acknowledged what the financial sector had long consigned to technical departments and internal security protocols.

Bank stability no longer depends only on capital, liquidity, credit quality and depositors' trust. It now also depends on the software the bank uses, the suppliers it relies on, the speed at which it can close vulnerabilities, and whether its systems can continue to operate when an attack unfolds not over days but within hours or minutes.

This is an important moment for the European financial system. For decades, central banks have maintained stability by monitoring capital, liquidity, non-performing loans, interest rates and market shocks.

They are now increasingly concerned about whether a bank can continue to operate if the software on which its business depends is attacked.

Risk no longer has to appear first in the balance sheet. It can originate in code, in a supplier, in a poorly patched system, in a shared software component used by several large banks, or in an attack that evolves faster than banking processes can keep up.

The ECB therefore did not react out of a fashionable fascination with artificial intelligence; it reacted because AI changes the speed of attack. Weaknesses in banking IT systems already existed. Cybercrime, digital blackmail, data theft, and attacks carried out by both criminal networks and states existed before artificial intelligence.

What is new is that the most advanced AI models can help attackers find vulnerabilities more quickly, prepare attack code faster, and test multiple capabilities at the same time.

Banks have always had to protect money. Now they must also protect the time they need to defend themselves.

A risk that is no longer purely technical

Banks have long distinguished between two types of risk. One was financial: bad loans, falling property values, loss of liquidity, market panic.

The second was operational: the danger that the bank could not function normally, that payments stopped, that clients could not access accounts, that data was lost or blocked, or that critical software, or a key supplier on which the bank depended, failed. Cyberattacks were generally seen as part of this second set of problems.

That division corresponds less and less to reality. If a cyberattack halts payments, blocks access to accounts, disrupts trading, compromises data, or brings down a key technology supplier, the consequences rapidly become financial.

When customers cannot access their money, a cyber incident ceases to be an internal technical problem for the bank. A much more serious question then arises: whether the bank can maintain its basic operations under the pressure of an attack.

> ECB's move shows that cyber security is no longer treated as a secondary function within the bank but is becoming part of financial stability

If the same weakness is found in other institutions or at a common supplier, the failure of one system very quickly becomes a wider problem of trust in the financial sector.

This is why the ECB's move is important: it shows that cyber security is no longer treated as a secondary function within the bank but is becoming part of financial stability.

A bank may have sufficient capital, strong liquidity and a sound loan portfolio, but if it cannot operate during a serious attack, its formal strength will mean little to customers, markets and regulators.

The European Systemic Risk Board, which monitors risks to the EU's financial system, warned on the same day that cyber risk to the EU's financial sector is no longer just a matter of isolated attacks on individual banks.

With the most advanced AI models, attackers can identify weaknesses more quickly and exploit them before banks can close them. This is why even a brief interruption in payment systems, access to accounts or at an important technology supplier can become a problem for several banks at the same time.

AI shortens the time for defence

The biggest change AI is bringing to cyberspace is not only that attacks can become more sophisticated. More importantly, it shortens the time between discovering a weakness and exploiting it.

Under the old regime, a bank could rely on a familiar cycle: vulnerability discovered, risk assessed, patch tested, solution implemented, system stability verified. That process was not perfect, but there was still room to respond.

AI reduces that margin. A model that can help a programmer write software can also help an attacker find weaknesses in software. A model that speeds up code analysis can also speed up attack preparation. A model that automates routine work can allow many more targets to be tested in much less time.

This does not mean that AI is breaking banks on its own, nor that every attack is automatically successful. It means that defenders have to work faster than before.

> A bank must know where its weak points lie, who maintains its systems, how quickly it can close a vulnerability, and how it will continue to operate if an attack does succeed

This is why the ECB is pushing for better vulnerability management, faster software patching, stronger monitoring of internet-exposed systems, improved attack detection, and more robust crisis recovery.

These terms may sound technical, but a simple logic lies behind them. A bank must know exactly what it is using, where its weak points lie, who maintains its systems, how quickly it can close a vulnerability, and how it will continue to operate if an attack does succeed.

For readers outside the banking and IT worlds, this can be reduced to a single image. In the past, a bank could rely on having enough time to lock a door once it learnt that the lock on that model of door was weak. Now there is a risk that thousands of such locks will be found, tested and attacked almost simultaneously.

In such a world, it is not enough to have a good door. One must know who made it, when it was last checked, who has the key, how quickly it can be repaired, and what happens if it does open.

Suppliers become the weak point in the system

The greatest vulnerability is often not in the bank itself. Large banks have been outsourcing parts of their operations to external technology companies for years.

They use cloud services, external software

platforms, security tools, consultants, data centres, open-source software components and numerous other services without which they cannot function. This has enabled them to develop faster and reduce costs. At the same time, it has created a dependency that is difficult to control.

If a large number of banks use the same supplier or the same software component, any weakness in that supplier is no longer just a single institution's problem. It becomes a shared risk, as an attack on such a point can affect several banks simultaneously.

Therefore, in the letter the ECB specifically requests that banks pay close attention to third-party suppliers, software components and outdated infrastructure.

> An old system that is difficult to maintain, slow to patch, and dependent on a small number of experts is a potential source of crisis

This will be one of the most challenging parts of the new regime for banks. It is not enough for a bank to strengthen its own IT team; it also needs to know how resilient its suppliers are. It must check whether they report vulnerabilities promptly, how they test their systems, whether they have a recovery plan, how transparent they are, and whether multiple large institutions depend on the same service.

In practice, this means tighter contracts, more demanding checks, higher costs and far less scope to postpone the modernisation of legacy systems.

Banks must accept that legacy software is no longer just an efficiency issue. In a world of AI-powered cyberattacks, it becomes a financial vulnerability.

An old system that is difficult to maintain, slow to patch, and dependent on a small number of experts is not just a technical problem; it is a potential source of crisis.

A quick defence carries its own risks

There is another part of the problem that is particularly unpleasant for banks. If they are slow to apply patches, they leave the door open to attackers. If they introduce patches too quickly, they risk breakdowns, errors and outages in their own systems.

Banking systems are not simple applications that can be changed without consequence. They process payments, loans, market transactions, customer accounts and data, where errors can have serious costs.

This means banks will have to learn to work faster without becoming careless. They will need to test more efficiently, isolate critical systems more effectively, automate some monitoring, and have a more secure fallback if a new patch causes a problem.

Cyber resilience will no longer be only about preventing attacks. It will also be about enabling the bank to defend itself without causing its own outage.

> UK supervision relies on working with the sector, identifying vulnerabilities and reviewing existing rules on the resilience of financial institutions

The Bank of England warned of the same problem in a July report but did not ask banks to submit specific action plans by a set date. For now, UK supervision relies on working with the sector, identifying vulnerabilities and reviewing existing rules on the resilience of financial institutions.

It is a softer approach than the one adopted by the ECB, but it is based on the same assessment. AI shortens the time attackers need to find and exploit a weakness, so banks can no longer rely on the pace of defence that was sufficient a few years ago.

That difference in approach will not remain

solely a European issue for long. Banks in London, Frankfurt, Paris and New York use the same technology providers, the same cloud platforms and often the same software components.

If a serious weakness emerges in a major supplier, it does not remain confined to one country or one regulator. Consequently, pressure on banks will increase outside the Eurozone, even where supervisors have not yet set a deadline such as the one set by the ECB.

After October, real supervision begins

The 31 October deadline marks the start of a new phase. Once banks have submitted their plans, the ECB will, for the first time, gain a clearer comparative picture of which institutions have serious weaknesses, which are slow to modernise, which are too dependent on suppliers, which lack sufficient staff to react quickly, and which still treat cyber risk as a technical liability rather than a stability issue.

After that, pressure will increase on the weakest organisations. It does not have to take the form of immediate fines. It is more likely to begin with additional questions, more rigorous checks, demands for clearer deadlines, pressure on management, and insistence that cyber resilience is funded as a core part of the business.

The regulator is no longer looking only at what is on the bank's balance sheet, but also at how reliable the digital layer is on which that balance rests

Banks that have postponed replacing old systems for years will find their excuses increasingly unconvincing. Those that have relied on suppliers without sufficient control will have to show that they understand where their real dependencies lie.

Protection costs will rise, particularly for banks that have delayed system modernisation for years. Technology providers will also come under greater pressure, as financial stability increasingly depends on companies that are not banks but without which banks cannot operate.

This is the most important consequence of the ECB's move. The regulator is no longer looking only at what is on the bank's balance sheet, but also at how reliable the digital layer is on which that balance rests.

A crisis of confidence in the financial system no longer has to begin with a withdrawal of deposits, a fall in share prices or a sharp rise in yields. It can also begin far more quietly, through a weakness in software used by multiple institutions, an attack on a supplier or failed incident recovery.

If a customer cannot access their money, payments do not go through, or multiple banks simultaneously depend on the same vulnerable technology, the line between a cyberattack and financial disruption blurs very quickly.

This is why the ECB's July decision is important, and why, in future, banking resilience will be measured by the system's ability to continue operating under attack.