Indonesia's OJK issues new cybersecurity rules after attacks escalate

Natasha Teja
10 January 2023

Jakarta (Credit: amadeustx on shutterstock)

Indonesia's financial regulator has issued banks with a new cybersecurity framework amid increasing attacks on the country's financial system – but practitioners warn further updates will be necessary to keep pace.

The Financial Services Authority (OJK) **issued** the framework on 27 December, outlining requirements for risk assessments as well as guidelines for incident reporting and risk management.

The cybersecurity regulations come after a rise in cyberattacks and threats in recent years specifically targeting the financial sector. According to Indonesia's National Cyber and Crypto Agency (BSSN), 920 million cyberattacks occurred in Indonesia in 2021 alone – with Indonesia's financial sector being the most targeted industry in the country, suffering over one in five of such attacks.

Most attacks were malware attacks, trojan activity and phishing attempts, the BSSN has said.

To mitigate these threats, the new OJK framework requires commercial banks to conduct an assessment of their inherent cybersecurity risks, taking into account four factors – technology, bank products, organisational characteristics, and cyber incident track records.

It instructs banks to establish governance frameworks, a cyber security risk control system and adequate human resources to support their cybersecurity risk management. The OJK has also instructed commercial banks to conduct regular cybersecurity testing based on vulnerability analyses.

"One challenge that banks will face is that there is a degree of prescription regarding how certain risk assessments need to be conducted within this regulation," says **Simon Onyons**, managing director for cybersecurity at FTI Consulting in London.

Onyons adds that this should not create issues "as long as firms are able to understand and integrate this risk assessment approach with their overarching enterprise risk assessment strategy".

A key aspect of the regulation is the provisions concerning incident reporting, which require banks to notify the OJK within 24 hours of "the earliest available information" regarding any cyber incident – although the regulator does not clarify what constitutes a cyber incident, or differentiate between threat levels.

"The detail is in the wording – a cyber incident must be reported within 24 hours 'after it is known'" explains Onyons. He says that deadline is reasonable, "so long as regulators understand that it can take time to reliably identify an incident as a cyber

incident, as opposed to other operational issues or loss events."

"The issue with incident reporting deadlines lies with the quantification of an incident," adds Onyons. "Firms need to have robust and tested incident response plans in place to identify quickly the source of business interruption or data loss. Where this is a cyber-related issue, this could arguably take longer than 24 hours."

The OJK's 24 hour deadline is the same as that required by its American and European counterparts. In the US, under the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA), any federal entity receiving a report on a cyber incident must share that report with the Cybersecurity and Infrastructure Security Agency (CISA) within 24 hours. Similarly, under the EU's Network and Information Security Directive (NIS 2.0), organisations must notify regulators of any breaches within 24 hours.

"The 24-hour reporting requirement is common practice under many national regulations in jurisdictions around the world," says **Denny Rahmansyah**, partner at SSEK. "The 24-hour reporting requirement is based on the principle that IT incidents should be shared as soon as possible to the extent permitted by law so that they can be assessed."

But the OJK framework omits guidance concerning customers' personal data, focusing instead on cyber incident prevention and reporting. The regulation does however warn that an employee's personal device that is connected to a bank's network poses an inherent risk. The OJK stated that "the greater the percentage of employees who have access through personal devices, the higher the bank's inherent risk."

Rahmansyah tells GBRR that another aspect lacking in the new regulations is the practice of information-sharing. "Many jurisdictions have put in place cybersecurity information-sharing mechanisms (mandatory or voluntary) to facilitate the sharing of cybersecurity information among banks, regulators and security agencies."

He adds, "These communications are established for multiple purposes, such as helping specific parties defend themselves against emerging cyber threats."

The OJK framework also prompts banks to regulate their third-party IT providers, requiring them to ensure they "have sufficient competence", which can be proven by "certification or recognition from an authorised institution in Indonesia or abroad".

Attacking Indonesia's IT Vulnerabilities

The OJK's cyber security and resilience framework was prompted by high-profile string of cyber-attacks affecting Indonesian banks and political institutions.

Recent high-profile incidents in the country have included a September 2022 attack in which a hacker with the pseudonym "Bjorka" leaked data from more than a billion registered Indonesian SIM cards. The hacker also released confidential documents between President Joko Widodo and Indonesia's State Intelligence Agency. A number of other senior public officials also fell victim to the data breach with their phone, identity, and vaccine numbers being made public.

The new OJK framework comes only a matter of months after it released a trio of new IT-focused operational resilience **requirements** in July, following a ransomware attack on Indonesia's central bank in December 2021.

That attack saw perpetrators allegedly steal non-critical employee data and deploy ransomware payloads on several devices on the Bank Indonesia network. However, the central bank stated that it was able to mitigate the attack before it affected services to the public.

According to data from Indonesia's Ministry of Communication and Information Technology (Kominfo), the country saw over 888 million recorded cyber threats in 2021, or 42 threats per second.

Onyons says the new framework will have to continuously evolve. "When cyber-attacks are successful, they tend to be repeated," he says. "Unless financial services firms continue to mature from a cyber resilience perspective, they will remain a lucrative and attractive target for attacks."

Natasha Teja

Author | Senior news reporter