CENTRE DE DROIT
BANCAIRE ET FINANCIER

Cyber attacks

New reporting obligation takes shape

Par Célian Hirsch le 27 May 2024

From 1 January 2025, banks, insurance companies and financial market infrastructures will have to report cyber attacks to the Federal Office for Cyber Security (FOCS) within 24 hours. The Federal Council has just put out to consultation the draft ordinance that implements art. 74a ff of the Federal Act on Information Security (obligation to report cyber attacks).

As we explained earlier (see Hirsch, cdbf.ch/1261), banks will now have to inform the OFCS in the event of a cyber attack. The new duty to notify the OFCS applies to all critical infrastructures. These include banks, insurance companies, financial market infrastructures and cloud providers (art. 74b ISL). In the draft cybersecurity ordinance (P-OCyS), the Federal Council proposes a number of exemptions for small infrastructures (art. 16 P-OCyS). However, these reliefs do not apply to banks, insurance companies and financial market infrastructures.

In the event of a cyber attack, banks could be required to inform three different authorities, namely FINMA, the FDPIC and the FOSC. A new Art. 39 para. 1 FINMASA, which will also come into force on 1 January 2025, provides that FINMA will be able to communicate to the FOCS certain information that the latter requires. For its part, the FDPIC will need the bank's agreement in order to communicate information to the OFCS.

Before announcing the cyber attack, the bank will have to examine whether the threshold for the duty to inform has been reached. This threshold is different for each of the three authorities (see table below). With Art. 18 P-OCyS, the Federal Council is attempting to clarify the four situations that trigger a duty to report to the FOCS (Art. 74d ISL). According to this provision, a cyber attack must be reported if it :

1. jeopardises the operation of the critical infrastructure concerned ;
2. has led to the manipulation or leakage of information ;
3. has gone undetected for a prolonged period, in particular if there are indications that it was carried out with a view to preparing further cyber attacks, or
4. is accompanied by blackmail, threats or coercion.

With regard to the content of the report, Article 74e of the ISL stipulates that it must include information on the authority or organisation subject to the obligation to report, the type and execution of the cyber attack, its effects, the measures taken and, if known, planned measures. The Federal Council specifies this content in Art. 19 P-OCyS, requiring in particular precise information on the cyber attack, such as the date and time of the detection of the attack, the

date and time of the attack, the type of attack, the methods of attack and data on the attacker. The Federal Council used FINMA Communication 05/2020 on the obligation to report cyber attacks in accordance with Art. 29 para. 2 FINMASA as a basis for determining the information to be transmitted to the FOCS.

The Swiss Bankers Association (SBA) had requested that FINMA Communication 05/2020 be adapted to the new obligation to report cyber attacks to the FOCS. Since then, the management of cyber attacks has been clarified in Circular 2023/1 on operational risks and resilience (cf. Hirsch, cdbf.ch/1265), but there is no indication that the duty to report to FINMA will be modified as a result of the new duty to report to the OFCS.

The summary table below provides an overview of the three separate reporting obligations in the event of a cyber attack :

Devoir d'annonce des cyberattaques

	FINMA	PFPDT	OFCS
Conditions	La cyberattaque vise des actifs d'importance critique et met en danger un ou plusieurs éléments faisant l'objet d'une protection (objectifs de protection) dans les fonctions d'importance critique et leurs processus.	La cyberattaque constitue une violation de la sécurité des données et entraîne vraisemblablement un risque élevé pour les personnes concernées.	La cyberattaque: -met en péril le fonctionnement de l'infrastructure critique concernée; -a entraîné une manipulation ou une fuite d'informations; -n'a pas été détectée pendant une période prolongée, en particulier si des indices laissent penser qu'elle a été exécutée en vue de préparer d'autres cyberattaques, ou -s'accompagne d'actes de chantage, de menaces ou de contrainte.
Délai	Annonce dans les 24 heures, puis annonce détaillée dans les 72 heures	Dans les meilleurs délais	Dans les 24 heures
Contenu	L'annonce doit contenir la nature de la cyberattaque, ses conséquences et les mesures prises ou envisagées (cf. les sources ci-dessous pour les différences selon l'autorité destinataire).		
Sources juridiques	Art. 29 al. 2 LFINMA Communication FINMA sur la surveillance 05/2020 Cf. ég. Circulaire 2023/1 sur les risques et résilience opérationnels	Art. 5 let. h LPD Art. 24 LPD Art. 15 OPDo	Art. 74*d* s. LSI Art. 18 p-OCyS

Cf. ég. HIRSCH CÉLIAN, Le devoir d'informer lors d'une violation de la sécurité des données, Avec un regard particulier sur les données bancaires, thèse, Genève 2023