Eidgenössische Finanzmarktaufsicht FINMA
Autorité fédérale de surveillance des marchés financiers FINMA
Autorità federale di vigilanza sui mercati finanziari FINMA
Swiss Financial Market Supervisory Authority FINMA

FINMA Guidance 05/2020

Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA

7 May 2020

Laupenstrasse 27
3003 Bern
Tel. +41 (0)31 327 91 00
Fax +41 (0)31 327 91 01
www.finma.ch

1 Introduction

FINMA continues to view the risk of cyber attacks[1] on the Swiss financial centre as very high. FINMA-supervised institutions are a target for cybercriminals, who not only have their sights on financial interests, but also target the availability, confidentiality and integrity of the critical technology infrastructure and sensitive information. Particularly in high-stress situations (such as the current COVID-19 pandemic), there is an increased risk of cyber attacks. Cybercriminals are utilising this time of uncertainty, adapting their attack strategies to the current situation and thereby placing an additional burden on already challenged firms.

FINMA is publishing this guidance to remind all supervised institutions of their legal requirement, pursuant to Article 29 para. 2 FINMASA, to immediately report any incident that is of substantial importance to the supervision. This encompasses significant incidents with regard to successful or partially successful cyber attacks.[2] FINMA will review the possibility of transferring the following clarifications to a circular at a later point in time based on experience.

2 Cyber attacks of substantial importance to the supervision

With reference to cyber attacks, the protection of individuals (i.e. creditors, investors and insured persons) and the proper functioning of the financial markets directly or indirectly[3] impacted by a cyber attack are of substantial importance.

FINMA's primary focus here is on the critical functions[4] of supervised institutions where successful or partially successful cyber attacks would lead to failure or malfunction. This may significantly impact the protection of individuals, potentially leading to the impairment of the protective goal of availability. Additionally, the protective goals of integrity and confidentiality of information or data can also be jeopardised by such attacks. If systemically important institutions or several institutions that provide critical interlinked

[1] Attacks from the internet and similar networks on the integrity, availability and confidentiality of the technology infrastructure, particularly in relation to critical and/or sensitive data and IT systems

[2] For insurance companies the reporting obligation is also inferred from the media impact and potential damage to reputation and solvency caused by cyber attacks. Margin nos. 1 and 5 FINMA Circ. 08/25 "Duty to inform – insurers".

[3] For instance, through attacks on critical infrastructures for the FINMA-supervised institutions (e.g. internet service providers, power producers etc.).

[4] Products or services of supervised institutions and their underlying business processes (e.g. payment transactions, cash supply, exchange trading, drafting and administration of insurance contracts, processing of claims and benefits, data management of particularly sensitive personal data in the health and life insurance branches; administration of securities and investments etc.) as well as their critical assets.

services are affected simultaneously, the proper functioning of Switzerland's financial markets could be put at risk under certain circumstances.

Cyber attacks are normally targeted directly at the supporting resources for these critical functions. Supporting resources that are designated as critical assets include personnel, technology infrastructure, information and facilities as well as critical service providers[5] who support the business processes of these critical functions. Every supervised institution must identify its critical functions, the corresponding business processes and supporting critical assets independently[6].

If a cyber attack on critical assets results in one or more of the protective goals of critical functions and their business processes being put at risk, this must be reported to FINMA immediately.

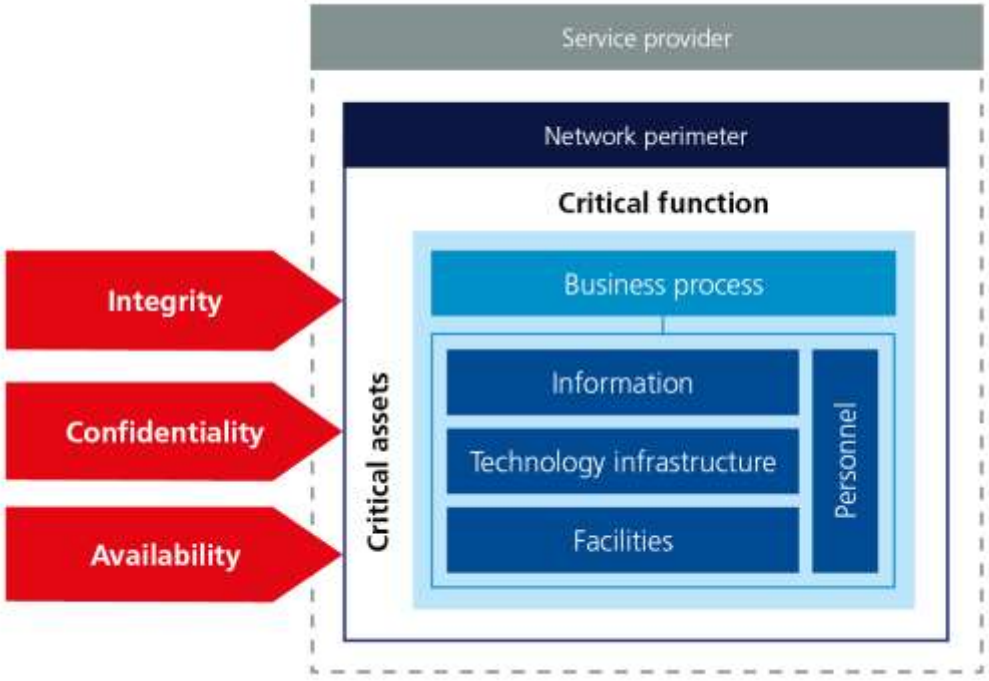

Figure 1: Diagram showing a cyber attack on the critical functions of a supervised institution.

A non-exhaustive list of critical assets and possible cyber attacks on them is provided in Annex 2.

[5] If an institution outsources key functions to other individuals or legal entities, the supervised institution is also responsible for reporting cyber incidents of its service providers, provided that there is a link to the outsourced key functions. See Article 47 para. 2 of the Insurance Supervision Act (ISA; SR 961.01)

[6] For example, margin no. 135.2 or margin no. 135.7 ff. FINMA Circ. 2008/21 "Operational risks – banks" or SIA Minimum Standards for Business Continuity Management, margin no. 28 ff. FINMA Circ. 2017/2 "Corporate governance – insurers"

3 Immediate reporting to FINMA

Immediate reporting to FINMA means that the affected supervised institution informs FINMA through the responsible *(Key) Account Manager* within 24 hours of detecting such a cyber attack and conducting an initial assessment of its criticality. The actual report should be submitted within 72 hours via the FINMA web-based survey and application platform (EHP)[7,8].

The following list contains guidance on the content of such a report to FINMA:

- Name of institution
- Contact person including contact details (telephone and email address)
- Date / time of report to FINMA
- Date / time when attack was discovered
- Date / time of attack (if already known)
- Description of cyber attack and current status
- Initial assessment of severity of the cyber attack (see Annex 1) *(selection: medium, high, severe)*
- Severity trend *(selection: decreasing, stable, increasing)*
- Affected entities (affected organisational unit(s) within the institution or service provider)
- Affected protective goals *(multiple selection: confidentiality, integrity, availability)*
- Affected critical functions, business processes or assets (affected information, technology infrastructure, facilities or personnel)
- Affected number of customers (current status)
- Vectors of attack (*multiple selection: email, web-based attack, brute force attack, identity theft, removable media, loss/theft of devices, exploitation of software vulnerability, exploitation of hardware vulnerability, other [please define])*
- Type of attack (description) (e.g. DDoS, unauthorised access, malware, misuse / improper use of technology infrastructure etc.)
- Administrative, operational and/or technical countermeasures with expected time to effectiveness
- Communication measures (what, to whom, when)

[7] https://www.finma.ch/en/finma/extranet/ehp-survey-and-application-platform/ (available starting from June, 1st, 2020)

[8] On the EHP platform: "EHP" – "Reports" – Button: "New report" – Reporting Template: "Report cyber attack"

If there are new developments or assessments related to the same attack after the reporting obligation has been met in full, a new report must be submitted within the specified deadline of 72 hours.

For cyber attacks with the severity levels high and severe (see Annex 1), once the institution has finished processing the case FINMA expects a conclusive root cause analysis to be submitted including an analysis, reason for the success of the attack, impact of the attack on the observance of regulations, operations and customers as well as mitigating measures to address the consequences of the attack. For cyber attacks with the severity level severe (see Annex 1), proof and analyses of the proper functioning of the crisis organisation must also be submitted.

For cyber attacks with the severity level medium (see Annex 1), a conclusive root cause analysis is sufficient.

FINMA expects the detailed requirements from the guidance on reporting cyber attacks to be implemented by 1 September 2020 at the latest or earlier on a best effort basis.

Annex 1: Determining the severity of a cyber attack

The following criteria can be applied as an initial assessment for determining the severity of a cyber attack:

Severity	Definition	Criteria
Severe	Extensive and prolonged damage to protective goals (availability, integrity, confidentiality) of critical assets present or expected.	– Availability: critical assets are not available in the medium to long term (failure > 200 % of the RTO[9]) – Confidentiality / integrity: sensitive information affected to (almost) full extent – Financial implications or damage to the institution's reputation endangering its existence – Overcoming the cyber attack requires the activation of the crisis organisation (BCM)
High	Protective goals (availability, integrity, confidentiality) of critical assets are substantially damaged or threatened.	– Availability: critical assets are not available in the medium term (failure >= RTO) – Confidentiality / integrity: sensitive information and / or critical information for the business process affected to a large extent – Considerable financial implications or damage to the institution's reputation – Overcoming the cyber attack requires the engagement of external resources.
Medium	Direct harm or threat to the protective goals (availability, integrity, confidentiality) of critical assets.	– Availability: critical assets are not available in the short term (failure > 50% of the RTO) – Confidentiality / integrity: sensitive information substantially[10] affected – Perceptible financial implications or damage to the institution's reputation – The cyber attacks can be overcome internally with the resources available.

[9] *Recovery Time Objective* – targeted duration of time for the restoration of critical assets

[10] Outside of 'business as usual'

Annex 2: Examples of critical assets and cyber attacks on their protective goals

	Examples of critical assets	Examples of cyber attacks
Information	Sensitive / confidential information such as e.g. customer identification data, insurance contracts, data in connection with the settlement of claims or benefits processing, minutes of meetings of the board of directors or executive board, strategy information, HR data etc.	Attacks on protective goals via unauthorised data access either from within the company or externally, leakage of data, data theft, alteration of data etc.
Technology infrastructure	Technology infrastructure necessary for performing a critical function (e.g. hardware, software, network infrastructure etc.)	Attacks on protective goals via (D)DoS, loss / theft of storage media with confidential information, ransomware etc.
Facilities	Essential facilities for the provision of critical functions (e.g. data centre, branches, back office premises etc.)	Attacks on protective goals by disrupting or deactivating the protective measures in place to regulate authorised access to sensitive areas etc.
Personnel	Employees who perform critical functions or contribute significantly to these such as e.g. executive board, traders, client advisers etc. as well as key personnel (e.g. employees with elevated rights, system administrators, security staff, accounting etc.)	Attacks on protective goals via social engineering (such as e.g. spear phishing), insider threats, identity theft, extortion etc.