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 03/2024

Findings from FINMA's cyber risk supervision, clarification of FINMA Guidance 05/2020 and scenario-based cyber risk exercises

7 June 2024

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

Contents

1 Introduction 3

2 Findings from cyber risk supervision 4

2.1 Outsourcing 4

2.2 Governance and identification 5

2.3 Protective measures 6

2.4 Detection, response and restoration 7

3 Clarification of FINMA Guidance 05/2020 8

4 Scenario-based cyber risk exercises 9

1 Introduction

Cyber risks have been among the main risks listed by FINMA in its annual Risk Monitor for many years. FINMA receives an ever-rising number of reports of successful or partly successful cyber attacks every year.

FINMA Guidance 05/2020 “Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA” sets out institutions’ reporting obligations in detail. The reports received since then reflect differing developments in the threat level, attack methods and targets of the attacks. FINMA’s supervisory work gives it a detailed picture of how supervised institutions deal with cyber risks. In particular, on-site reviews with a cyber-specific focus enable FINMA to assess the maturity of supervised institutions’ cyber defence measures in greater depth. The institution specific findings resulting from these reviews have been published on an aggregated basis in the FINMA Risk Monitor and the FINMA Annual Report.

This guidance is intended to give supervised institutions specific information on how to manage cyber risks based on these findings. It is relevant for all institutions supervised by FINMA. At several points the guidance makes explicit reference to FINMA Circular 23/1 “Operational risks and resilience – banks”. This information is primarily intended for the institutions to which this circular applies, but can also be used as a guideline by other institutions.

The guidance also deals with common questions about FINMA Guidance 05/2020 “Duty to report cyber attacks pursuant to Article 29 para. 2 FINMASA”.

Finally, the guidance discusses and provides further clarification on margin no. 70 of FINMA Circular 23/1.

2 Findings from cyber risk supervision

2.1 Outsourcing

As long ago as the 2020 Risk Monitor, FINMA reported an increase in successful attacks on the supply chains of supervised institutions, accounting for around 25% of all attacks. This rose to over 50% in the following years and has remained at around this level. FINMA has therefore taken a closer look at the issue of outsourcing-related cyber risks[1] and made this into a focus of its supervision. FINMA's aim was to find out why attacks on service providers had an above average chance of success. On-site reviews showed that unclear cyber security requirements for service providers and either an absence of audits, or a lack of regular assessments of these requirements by supervised institutions, were among the main reasons:

- After serious security failings were identified, very few institutions proactively engaged with their most important service providers to ensure they mitigated this vulnerability quickly and before any damage occurred.
- FINMA often observed that the directly supervised institutions quickly brought serious vulnerabilities under control and were therefore able to avoid a direct loss. However, often their service providers did not deal with the issue as effectively and were not well prepared enough for successful cyber attacks.
- Very often the supervised institutions did not have a full inventory of their service providers. They did not have information about whether critical data was stored at a service provider or they were performing a critical function. Hence supervised institutions often only carried out insufficient audits, or no regular assessments at all, of such service providers.
- As far as inventories of the main subcontractors in outsourced functions were concerned, there were major differences between the institutions in how developed their systems were to record, document and access critical data.[2]
- The institutions concerned had in many cases not defined clearly what represents critical data for them. This made it much more difficult not just to protect this data internally, but also to appropriately classify the service providers and determine the control measures needed to reduce the risks that were identified.

[1] See the addition of outsourcing as a main risk in the 2023 Risk Monitor and the discussion in the 2023 FINMA Annual Report.

[2] See also margin no. 14 FINMA Circular 18/3.

If an institution outsources a significant function to a service provider (particularly critical functions or critical data to a material degree), the service provider must meet the same regulatory requirements as the supervised institution. The same requirements apply to any subcontractors. Hence FINMA regards an up-to-date inventory of all significant outsourced functions including subcontractors as an essential tool for supervised institutions to possess.

The institution remains responsible for complying with the supervisory requirements at all times. This responsibility cannot be outsourced or transferred to a service provider.

2.2 Governance and identification

Governance in dealing with cyber risks is a further critical issue. In the past FINMA has often observed that cyber risks were depicted as a purely technological problem and were therefore not given the necessary priority at management or board level. Hence the new FINMA Circular 23/1 clearly defines the responsibilities of the board of directors and executive board, e.g. for banks (see margin no. 61). FINMA also identified the following additional weaknesses in governance at many supervised institutions:

- At medium-sized institutions there was often no clear differentiation between the operational management of cyber risk and the independent control body. It is essential that the effectiveness of operational management is continually reviewed by an independent control body.[3]
- Identification of the institution-specific cyber risk threat landscape was often inadequate. Moreover, it was often unclear which staff had access to critical data, as there was no central authorisation tool. This made it more difficult for the institution's security organisation to draw up protective measures for critical data.
- A large number of supervised institutions failed to explicitly integrate cyber risks into their overall management of operational risk. As a result it was not possible to ensure cyber risks were being managed systematically and comprehensively.
- In addition, a number of supervised institutions did not sufficiently define cyber risks and their corresponding risk appetite and risk tolerance. However, these are central components of an effective policy to protect against cyber risks.

[3] See the sections on control functions and independent control bodies in FINMA Circulars 2017/1 "Corporate governance – banks" and 2017/2 "Corporate governance – insurers".

As discussed in the FINMA Risk Monitor, cyber risks have been among the main risks for supervised institutions for years, which is why it is essential for institutions to recognise them as a separate risk category in the management of qualitative operational risks and define a corresponding risk appetite and risk tolerance.

It is also essential that key controls of cyber risks conforming to internationally recognised standards or practices are integrated into the internal control system (ICS) and their effectiveness is regularly reviewed, evaluated and documented by an independent control body. The separation of tasks, competencies and responsibilities to ensure independence and prevent conflicts of interest also needs to be reviewed regularly.

2.3 Protective measures

As far as protective measures are concerned, ongoing supervision has noted a positive trend in recent years. For example, supervised institutions have put better and increasingly effective protective measures in place to defend against distributed denial of service attacks.[4] However, significant vulnerabilities were also found in this area:

- The protective measures on *Data Loss Prevention* (DLP) were often limited to customer identification information or credit card numbers and did not cover other critical data such as sensitive personal data, business secrets, intellectual property etc.
- Almost all institutions reviewed by FINMA had produced guidelines and processes on data backup and defined data recovery plans. However, some institutions did not test these processes against the scenario of a serious cyber attack, e.g. by malicious encryption software (ransomware).
- There is also potential for improvement in the area of cyber training and awareness at a large number of supervised institutions. In order for protective measures to be effective, it is essential that employees at all levels of the hierarchy are regularly informed about and trained on cyber risks, know and understand the most common methods of attack such as phishing and know who to contact within the company if they spot any signs of a cyber attack. This objective can be achieved, for example, by regular testing of staff on the topic.

[4] DDoS attack: A large number of enquiries from a distributed network of computers is used to overload a system (e.g. a website).

For institutions to which FINMA Circular 23/1 applies, the requirements for cyber risk training and awareness are explicitly listed in the Circular (see margin no. 26).

In addition it is essential for all institutions to test a scenario where an attacker manages to circumvent the protective measures and is able to cause maximum damage to the company. It is important to test backup and recovery strategies to determine whether, e.g. in the event of a complete encryption of critical data, it could be restored with the required timeliness, integrity, quality and completeness within the required deadlines. In this context we refer in particular to the new supervisory requirements for banks to maintain operational resilience in accordance with FINMA Circular 23/1.

2.4 Detection, response and restoration

The ability to identify cyber attacks quickly, detect and respond to them is an area that FINMA focuses on in most of its on-site reviews of cyber risk and is also often the subject of in-depth reviews.

During these on-site reviews FINMA often observed the following recurrent patterns at the supervised institutions:

- Some of the institutions only have incomplete response plans, or no plans at all, for cyber incidents or do not review the effectiveness of these plans.
- With respect to logging and detecting cyber attacks, the reviews also found that a number of institutions were failing to monitor their IT and communications technology promptly and systematically. In some cases critical log data was not being analysed, or was only analysed during office hours.
- Most institutions had measures in place to ensure the prompt restoration of normal business operations following exceptional outages. However, they often did not have specific restoration measures after cyber attacks.

Risk-oriented and scenario-based preparation by supervised institutions for cyber events and crises is essential. Preparing realistic response plans and testing them is an important determinant of being able to master stress situations resulting from cyber attacks effectively. In particular, it is extremely important to draw the relevant lessons and implement improvements immediately after a successful cyber attack.

3 Clarification of FINMA Guidance 05/2020

Since all supervised institutions were reminded of their obligation to report cyber attacks in FINMA Guidance 05/2020, FINMA has received a number of enquiries about how the guidance should be interpreted.

We are therefore clarifying the following points here:

- The institution has 24 hours from the time a cyber attack is discovered to submit an initial report to FINMA.
- Within these 24 hours supervised institutions are expected to make an initial assessment of the cyber attack's criticality to determine whether it meets the materiality threshold to be reported to FINMA.[5]
- For the initial report within 24 hours FINMA expects the supervised institution to notify their *key account manager* by email, telephone or in another suitable manner. This notification should contain an initial assessment of criticality and describe concisely the facts established so far. A completed form in the web-based survey and application platform (EHP) is not required at this point.
- Institutions which are also subject to the reporting obligation under the Information Security Act (ISA; RS *128*) may submit their 24-hour notification via the reporting form of the National Cyber Security Centre (NCSC) and select the option to forward the report to FINMA, provided this can be done within the deadline. The full 72-hour notification must still be submitted via the EHP.
- If an institution needs to decide whether to complete the determination of severity for an initial assessment or adhere to the 24-hour deadline, it should prioritise complying with the deadline.
- An initial report notified to FINMA within 24 hours can be withdrawn again at any time if the institution ultimately concludes after further investigation of the severity of the cyber attack that it did not meet the materiality threshold.
- If an institution's service provider (e.g. a hospital, asset manager, law firm) is not a material outsourcing partner within the meaning of FINMA Circular 18/3 "Outsourcing", the institution must ensure – based in particular on Article 22 Insurance Supervision Act, margin no. 68 FINMA Circular 23/1 and FINMA Guidance 05/2020 – that it is informed by the service provider about cyber incidents the provider suffers. If the institution classifies a cyber incident reported to it as relevant within the meaning of FINMA Guidance 05/2020, it must also submit the required reports to FINMA in such cases.
- The reporting deadlines of 24 and 72 hours are only counted on official bank working days. Cyber attacks with the severity level "severe" are an

[5] See FINMA Guidance 05/2020, Annex 1.

exception. These must be reported to FINMA within 24 hours, even outside of bank working days.

- The reporting obligation for outsourced functions is as follows: in accordance with margin no. 23 FINMA Circ. 18/3, supervised institutions have the same responsibility to FINMA as if they were performing the outsourced function themselves. This means in turn that the reporting period begins as soon as the institution, or the third party provider for outsourced functions, identifies a cyber incident. This also ensures that institutions who have not outsourced any functions receive equal supervisory treatment.
- In accordance with FINMA Guidance 05/2020, for reports on cyber attacks with "medium" severity, a concluding root cause analysis is required, comprising at a minimum the internal or external investigation and forensic report. For reports on cyber attacks with a "high" or "severe" degree of severity, the root cause analysis should comprise the following:
  - Reason for the success of the cyber attack;
  - Impact of the attack on compliance with supervisory requirements, the institution's operations and customers;
  - Mitigation measures taken to address the consequences of the attack.

  For "severe" cyber attacks, proof and analysis of the proper functioning of the crisis organisation must also be submitted.

4 Scenario-based cyber risk exercises

Institutions to which FINMA Circ. 23/1 applies must carry out risk-based and scenario-based cyber exercises in accordance with margin no. 70 of the Circular. The content and scale of these exercises is based on the principle of proportionality. For systemically important institutions, FINMA regards red teaming exercises[6] as an essential component of cyber risk exercises. Non-systemically important institutions should carry out at least one tabletop exercise[7] every year.

Institutions in supervisory categories 4 and 5 can meet this obligation by taking part in the exercises run by the Swiss Financial Sector Cyber Security Centre (Swiss FS-CSC).[8] Every participating institution must ensure that the institution-specific threat landscape of these exercises is documented transparently and the institution-specific findings from the exercises are

[6] Red teaming: security experts take on the role of an attacker and attempt to attack and breach a company's cyber security defences by replicating the attack methods of a malicious hacker.

[7] Tabletop exercise: simulating and playing through a scenario on paper.

[8] See https://fscsc.ch/.

reported. If the institution-specific threat landscape cannot be derived from the Swiss FS-CSC's cyber risk exercise, for example because the test scenario has limited relevance for an institution's cyber risk profile, the institution must still carry out an individual scenario-based cyber exercise to address the requirements of margin no. 70.

FINMA reserves the right to selectively carry out such risk-based and scenario-based cyber risk exercises selectively as part of the supervisory review or additional audit and monitor them closely. Established frameworks[9] should be used as a basis for the exercises.

[9] Such as TIBER-EU, CBEST threat intelligence-led assessments.