BÄR & KARRER BRIEFING JUNE 2024

FINMA'S CYBER RISK SUPERVISION: WHAT YOU NEED TO KNOW AND DO

A few days ago, on 7 June 2024, the Swiss Financial Market Supervisory Authority (FINMA) released its Cyber-Risk Guidance 03/2024, which summarises key findings from FINMA's cyber risk supervisory activities and clarifies the reporting obligations for cyber attacks. The Cyber Risk-Guidance expresses FINMA's interpretation of applicable law and should therefore be complied with by supervised institutions.

This briefing analyses the implications of the Cyber Risk-Guidance for supervised institutions and provides practical recommendations on how to comply with the regulatory requirements and manage cyber risks effectively.

FINMA'S EMPIRICAL FINDINGS FROM ITS CYBER RISK SUPERVISION

FINMA employs a variety of tools in its supervision of cyber risks. These include regular **risk assessments**, **on-site and in-depth reviews** and **scenario-based cyber exercises**. Through these tools, FINMA obtains a detailed picture of the cyber risk management and resilience of institutions under its supervision and identifies best practices and areas for improvement.

The newly published Cyber Risk-Guidance summarises key findings from FINMA's supervisory activity in the past years, highlighting recurrent shortcomings.

OUTSOURCING

FINMA has observed an **increase in successful attacks** on the **supply chains** of supervised institutions, which accounted for over 50% of all attacks in recent years. FINMA found that these attacks succeeded due to **unclear cyber security requirements** for service providers and a **failure** by supervised institutions **to audit** or at least **regularly assess** these requirements.

Very often supervised institutions did **not** have a full **inventory** of their service providers and **failed** in many cases to **define** clearly what constitutes **critical data** for them. This made it difficult to classify the service providers appropriately and to determine the control measures.

GOVERNANCE AND IDENTIFICATION

FINMA has also oberserved that governance in dealing with cyber risks is a further critical issue. Cyber risks were **often treated as a**

purely technical problem and did **not receive** the **necessary priority** at **management** or **board** level. FINMA has therefore defined the responsibilities for governing bodies and management in its revised circular 2023/1 "Operational Risks and Resilience – Banks" which came into force on 1 January 2024.

The Cyber Risk-Guidance also notes other common weaknesses in the governance of cyber risks, such as the **lack of clear separation** between the **operational management** of cyber risk and the **independent control function**, the **inadequate identification** of the **institution-specific cyber risk threat landscape**, the **failure to integrate cyber risks into the overall management of operational risks** and the **insufficient definition** of **cyber risks** and their corresponding **risk appetite** and **tolerance**.

PROTECTIVE MEASURES

FINMA has noted a **positive trend** in the measures taken by supervised institutions to protect themselves, particularly with regard to defence against **distributed denial-of service attacks** (**DDoS**) and setting up **data backup and recovery guidelines and processes**.

However, FINMA also identified **significant vulnerabilities**, such as the limited scope of **data loss prevention** (**DLP**) measures, the **lack of testing of backup and recovery processes** in case of a serious cyber attack (e.g., a ransomware attack) and **insufficient cyber training and awareness** among staff at all hierarchical levels.

DETECTION, RESPONSE AND RESTORATION

The ability to identify, detect and respond to cyber attacks in a timely manner is a **focus** of most of FINMA's cyber risk **on-site reviews**.

During these reviews, FINMA observed the following recurring patterns among the supervised institutions: some of them had **no or incomplete response plans** for cyber incidents or did **not test them for their effectiveness**, some of them did **not monitor** their IT and communications technology systematically and promptly, and some of them **lacked specific recovery measures after cyber attacks**.

CLARIFICATIONS ON FINMA GUIDANCE 05/2020

Following several enquiries from supervised institutions, FINMA also provides in the Cyber Risk-Guidance some clarification on the interpretation of FINMA Guidance 05/2020 regarding the cyber attack reporting duty under art. 29 para. 2 of the Financial Market Supervision Act (FINMASA).

REPORTING, PRIORITY AND DEADLINE CALCULATION

Within 24 hours of discovering a cyber attack, supervised institutions are expected to make an **initial assessment** of the attack's criticality and, if required, must **submit** an **initial report to FINMA**. Notification can be made via email, telephone or other suitable means. A completed form in the web-based survey and application platform (EHP) provided by FINMA is not required initially. An initial report submitted to FINMA can be **withdrawn** at any time if the institution concludes after further investigation that the incident should not have been reported.

Institutions subject to the Information Security Act (**ISA**) may **submit their initial report** through the reporting form provided by the **National Cyber Security Centre (NCSC)**, choosing to **forward it to FINMA**, if this can be done within 24 hours.

A completed form in the EHP must be submitted within **72 hours**.

In addition, FINMA made it clear that **meeting the 24-hour deadline** takes **precedence over completing the criticality assessment** and that, while reporting deadlines are generally based on official bank working days, in case of "**severe**" attacks a **strict 24-hour deadline** applies.

SERVICE PROVIDERS AND RESPONSIBILITIES FOR OUTSOURCED FUNCTIONS

The Cyber Risk-Guidance outlines how institutions have the **same reporting obligations for outsourced functions** as if they were performed in-house. Therefore, the **reporting periods begin** when the **institution**, or the **service provider** for the outsourced function, **identifies a cyber incident**.

However, this does **not apply** if a service provider does **not perform a significant function** (and is therefore not a material outsourcing partner). In such a situation, the institution must ensure that the **service provider informs** it of any cyber incidents the service provider suffers. If the institution classifies a reported incident as relevant under FINMA Guidance 05/2020, the **institution must report** the incident to FINMA.

ROOT CAUSE ANALYSIS

In case of a "**medium**" attack, supervised institutions must conduct a root cause analysis, including at least an **internal or external investigation** and **forensic report**.

For "**high**" or "**severe**" attacks, the analysis must also include the **reason(s)** for the attack's success, **impact on compliance, operations** and **customers**, **mitigation measures taken** and, for "severe" attacks, **proof of the crisis organisation functionality**.

The severity of an attack (severe, high or medium) needs to be assessed based on the critieria set out in Annex 1 to FINMA Guidance 05/2020.

PRACTICAL RECOMMENDATIONS

Based on its empirical findings from the cyber risk supervision described above, FINMA provides supervised institutions in the Cyber Risk-Guidance with recommendations on how to deal with cyber risks. This is particularly relevant from a practical perspective as FINMA recommendations carry significant practical weight. The main actions that supervised institutions may need to take now are the following (in addition to FINMA's recommendations in the Cyber Risk-Guidance, which are marked as such in brackets, we have included further recommendations based on our practical experience):

REVIEW OF OUTSOURCED FUNCTIONS

- **Regularly review** (at least **significant**) **outsourced functions** and ensure that the outsourcing arrangements include clear and specific **cyber security obligations and controls** for the service providers, **service levels**, **reporting mechanisms** and allow the outsourcing institution to **monitor** and **audit** their performance and compliance.
- Keep a complete and up-to-date **inventory** of all significant outsourced functions including subcontractors (as FINMA recommends in the Cyber Risk-Guidance).
- **Actively manage the risks** associated with each service provider by conducting **due diligence** and **risk assessments** of service providers and subcontractors before engaging them and on an ongoing basis to evaluate their cyber security posture and compliance with industry standards.
- Implement a **continuous monitoring strategy** to ensure that any changes in the service providers' operations or security practices are promptly identified and managed.
- Establish **clear communication channels** with all service providers for the timely exchange of information regarding cyber threats and incidents.
- Consider **contingency plans** and alternative solutions in case of a disruption of service providers.

IDENTIFICATION AND MANAGEMENT OF CYBER RISKS

- Identify cyber risks as a **distinct risk category** and integrate it in the management of qualitative operational risks and also define a corresponding **risk appetite** and **tolerance** (as FINMA recommends in the Cyber-Risk Guidance).
- Ensure that the **risk appetite** and **tolerance** for cyber risks are aligned with the institution's **strategic objectives** and are **communicated** effectively **across the organisation**.
- Integrate **key controls** based on internationally recognised standards or practices into the institution's internal control system (**ICS**) and **regularly assess** and **document** their effectiveness through an independent control body (as FINMA recommends in the Cyber-Risk Guidance).
- Develop a **comprehensive cyber risk assessment framework** that includes not only qualitative but also quantitative measures to better understand the potential impact of cyber risks.
- Integrate cyber risk management into the overall **risk management framework** to ensure a holistic approach to identifying, assessing and mitigating risks.

IMPROVEMENT OF PROTECTIVE MEASURES

- Improve **protective measures**, in particular **prepare** for scenarios in which attackers manage to bypass protective measures causing maximum damage (as FINMA recommends in the Cyber-Risk Guidance).
- **Test backup and recovery processes** to ensure operational resilience (as FINMA recommends in the Cyber-Risk Guidance).
- Engage in regular **cyber training and awareness for all employees**, not only IT staff, to ensure they are aware of their role in maintaining cyber security and can recognize and respond to potential threats (as FINMA recommends in the Cyber-Risk Guidance).
- Adopt a **layered security approach** that includes a combination of **preventive**, **detective** and **corrective controls** to provide a robust defense against cyber threats.
- Implement **advanced threat intelligence solutions** to stay ahead of emerging threats and to understand the tactics, techniques and procedures used by attackers.

ENHANCEMENT OF DETECTION, REACTION AND RECOVERY CAPABILITIES

- Prepare **realistic** (risk-oriented and scenario-based) **response plans** and **test** them (as FINMA recommends in the Cyber-Risk Guidance).
- Create an **incident response team** with clearly defined roles and responsibilities, ensuring that team members are trained and equipped to handle a variety of cyber incidents.

- Conduct regular **cyber incident response drills and simulations** to test the effectiveness of response plans and to identify areas for improvement.
- Develop a **security operations centre (SOC)** that operates around the clock to monitor, detect and respond to cyber incidents in real-time.
- Ensure **complying with** the **strict 24-hour deadline** for reporting **severe** attacks to FINMA (if in doubt, assume that the attack is severe and report it – the initial report can be withdrawn at any time).
- **Learn** from successful cyber attacks (as FINMA recommends in the Cyber Risk-Guidance). For this purpose, implement a **structured process for capturing lessons learned from cyber incidents**, both internal and external, and use this information to strengthen the cyber security posture.
- **Implement improvements** immediately after an attack.
- Regularly **review and update** cyber security **policies**, **procedures** and **controls** to reflect the evolving threat landscape and lessons learned from past incidents.

Please note that the Cyber Risk-Guidance does not cover all aspects or scenarios of cyber risk management, and it may be subject to change in the future. Supervised institutions should also be aware of the other applicable laws and regulations that may affect their cyber risk management, such as the Information Security Act, the Data Protection Act, the Banking Act or the EU NIS 2 Directive.

AUTHORS

Dr. Christian Kunz

Partner

christian.kunz@baerkarrer.ch

T: +41 58 261 52 66

Christian Kunz co-heads Bär & Karrer's Data Protection & Digital Economy as well as Technology, Media & Telecommunications (TMT) practice groups. He is an expert in the field of data, data protection, cyber security and technology law. He advises clients on data strategies and related processes, the use and monetisation of data, (cloud) outsourcings, international data transfers, data disclosure requests, and data breach incident management and recovery. He also advises on data-driven business models and platform solutions (XaaS, cloud services, IoT) and advanced technology projects (AI, Machine Learning, etc.)

Ferdinand Rombach

Associate

ferdinand.rombach@baerkarrer.ch

T: +41 58 261 54 12

Ferdinand Rombach is an associate at Bär & Karrer in Zurich. He primarily advises clients in the areas of data, data protection, cyber security and technology law. He also assists companies in internal investigations, especially with regard to regulatory enforcement-proceedings and cross-border white collar crime matters. Ferdinand studied law at the University of Mannheim and is admitted to the bar in Germany.

Dr. Katharina Schreiber

Associate

katharina.schreiber@baerkarrer.ch

T: +41 58 261 52 82

Katharina Schreiber is an associate at Bär & Karrer in Zurich. She is mainly active in the area of data protection & digitalisation, in particular with a focus on the EU law aspects of the Swiss data protection legal framework in client support. Katharina studied law at the University of Passau and holds both German state examina.

CONTRIBUTORS

Lars Seifert, Chief Information Security Officer