

Cybersecurity and operational resilience

*Dr Alexander Ressos, TEP
Attorney-at-Law (Switzerland), Solicitor (Hong Kong),
Solicitor (England & Wales)*

Digitalisation has a counterpart: vulnerability. Financial institutions are the preferred targets of cyberattacks, whether by ransomware, phishing or the compromise of suppliers. The Geneva financial centre, with its wealthy clients and its commodity traders, is a prime target. Through its circular on operational risks, FINMA requires supervised institutions to manage IT risks and to report serious cyberattacks within twenty-four hours. In 2025 the Confederation introduced a general obligation to report cyberattacks against critical infrastructure.¹ The known cases, several of which affected institutions in French-speaking Switzerland, show that successful attacks often target the institution's service providers, whose security was less closely monitored than that of the institution itself.²

Operational resilience goes beyond cybersecurity alone. It concerns an institution's ability to maintain its critical functions in the event of an outage, an attack, the failure of a supplier or a disaster. It presupposes the identification of those functions, scenarios, testing and recovery plans. The European Union has adopted a regulation on digital operational resilience, applicable since January 2025, which imposes detailed requirements on institutions and their critical IT service providers. Geneva institutions that belong to European groups or serve clients in the Union feel its indirect effects.³ The concentration of cloud service and banking system providers among a few companies, almost all of them American, moreover creates a dependence that the Swiss and European authorities now regard as a systemic risk.

Caution. Outsourcing IT to cloud service providers transfers the execution, but the responsibility remains. The institution remains responsible to its clients and to FINMA for the confidentiality, availability and integrity of the data, including where the provider is established abroad and subject to laws that may require it to disclose data to the authorities of its own country.

1 Notes

1. FINMA Circular 2023/1 “Operational risks and resilience – banks”, which replaces Circular 2008/21 and has been in force since 1 January 2024 (The Governance Law Firm, “Révision de la FINMA : circulaire Risques et résilience opérationnels – banques”, thegovernancelawfirm.com); obligation to report cyberattacks against critical infrastructure to the National Cyber Security Centre within twenty-four hours, based on the Information Security Act and in force since 1 April 2025, with sanctions from 1 October 2025 (NCSC, “L’obligation de signaler les cyberattaques contre des infrastructures critiques entre en vigueur le 1er avril 2025”, bacs.admin.ch). ↩
2. FINMA, dossier “Cyber risks (2024)” and press release of 7 June 2024 on supervisory communication 03/2024 (finma.ch): a 30 per cent increase in reports of successful or partially successful cyberattacks in 2024 compared with the previous year; ransomware (the PLAY, AKIRA and Lockbit 3.0 groups), business e-mail compromise, waves of denial-of-service attacks and supply-chain attacks, the latter representing nearly one third of the incidents reported; more than half of the attacks reported in 2022-2023 concerned outsourced services; reporting obligation based on Art. 29 para. 2 FINMASA; more than a dozen on-site inspections devoted to cyber risk in 2023. ↩
3. Regulation (EU) 2022/2554 of 14 December 2022 on digital operational resilience for the financial sector (DORA), applicable since 17 January 2025: IT risk management, incident reporting, resilience testing, third-party provider risks; Autorité de contrôle prudentiel et de résolution, “Digital Operational Resilience Act (DORA)”, acpr.banque-france.fr (accessed September 2026). ↩

For general information only. This article does not constitute legal or tax advice, does not replace advice on an individual case and creates no lawyer-client relationship. It reflects the legal position as of September 2026.

Online version: helveticaregister.com/geneva-cybersecurity-and-operational-resilience