

Security and cyber risks

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

The concentration of valuable companies and wealthy individuals in a small canton creates security risks. Cyber attacks against Swiss companies and authorities have increased in recent years. In 2023, an attack on an IT supplier of the federal administration exposed sensitive data of federal authorities.¹ Commodity traders, crypto companies and wealth managers are attractive targets for criminals and state actors, since they hold valuable data and assets. The crypto industry has suffered several hacks in which tokens worth millions were stolen.

While the canton and the companies have invested in cyber security, the Confederation has created a Federal Office for Cyber Security.² The protection of wealthy residents and their families is a further concern, handled by private security firms and the police. These risks are unlikely to change the location decisions of most companies, but they add to the costs of operating in the canton. A major cyber incident affecting the financial or commodity infrastructure could damage the canton's reputation for security and stability.

1 Notes

1. Federal Council, press release "Hackerangriff auf Firma Xplain: Bundesrat mandatiert politisch-strategischen Krisenstab 'Datenabfluss'", 28 June 2023, admin.ch: ransomware attack on the IT service provider Xplain affected data of the federal administration; Federal Office for Cyber Security (BACS), press release "Hackerangriff auf Firma Xplain: Bericht ... zur Datenanalyse publiziert" (2024), ncsc.admin.ch: data published on the darknet by the group "Play" on 14 June 2023, about 1.3 million objects, of which about 65,000 relevant to the federal administration. ↩

Security and cyber risks

2. Federal Council, press release "Meldepflicht für Cyberangriffe auf kritische Infrastrukturen", 7 March 2025, admin.ch: operators of critical infrastructure must report cyber attacks to the Federal Office for Cyber Security (BACS) within 24 hours, from 1 April 2025. BACS operational since 1 January 2024 as successor of the NCSC (Federal Council decision of 2 December 2022; de.wikipedia.org, "Bundesamt für Cybersicherheit"). ↩

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/zug-security-and-cyber-risks