KESSLER

Cyber Message 2025

Risk and Insurance

A SECURE FUTURE.

Geopolitical tensions, hybrid warfare and AI-driven attacks are shaping the global cyber risk environment in 2025. These developments are affecting Switzerland, too. New reporting obligations are intended to actively strengthen the protection of companies and authorities. But in which areas does an in-depth review need to be carried out? Kessler shares its experience to illustrate the relevance of this for corporate security. Integration into risk management is essential for increasing resilience in a targeted and sustainable manner.

Changes in the law

REPORTING OBLIGATION FOR OPERATORS OF CRITICAL INFRASTRUCTURE

Since 1 April 2025, operators of critical infrastructure have been obliged to report cyber incidents in Switzerland. The sectors affected by this law include energy, transport, healthcare, finance and public administration. Cyberattacks must be reported to the National Cyber Security Centre (NCSC) within 24 hours if the functionality of critical infrastructure is restricted, a data leak occurs or there is an incident involving extortion or coercion. If the report is not submitted, authorities and organizations subject to reporting requirements face fines of up to CHF 100,000 as of October 1, 2025. The basis for this is the amendment to the Information Security Act (FAISC), which is intended to increase the resilience of critical infrastructure.

ARTIFICIAL INTELLIGENCE

AI agents speed up processes and optimize decisions but harbor significant cyber risks. Manipulated training data, unclear responsibilities and uncontrolled actions increase the potential for abuse. The EU Artificial Intelligence Act adopted in 2024 establishes clear rules: AI agents in sensitive areas such as credit checking or human resources are considered high-risk systems with strict requirements regarding transparency, control and risk management. Providers of generative base models are subject to additional requirements in terms of robustness and documentation, including Swiss companies with a connection to the EU.

Small-scale providers see barriers to innovation, while multinational companies warn of regulatory complexity and high costs. All call for more precise guidelines and longer transitional periods. In parallel to this are voluntary codes of conduct and standards (e.g., CEN, ETSI) that are being developed. Switzerland is also planning its own legal framework – based on that of the EU – to be implemented by 2026. The focus is on AI agents that act autonomously or interact with customers. Those that wish to use them productively need technical expertise and regulatory foresight: risk management, transparent processes and internal controls are becoming mandatory – as well as a competitive advantage.

Current risks

CYBERSECURITY IN M&A TRANSACTIONS

Cybersecurity often receives too little attention when it comes to M&A activities. According to IBM, more than half of companies only consider cyber risks after completing their due diligence. However, such risks need to be identified and quantified at an early stage and in a targeted manner by analyzing the target infrastructure and continuously assessing the business impact in the transaction cycle. This is the only way to secure returns and protect value in the long term.

Together with Marsh, Kessler identifies the target's vulnerability worldwide and assesses the financial consequences of outages, data breaches and ransomware attacks. The results flow into a structured report with prioritized recommendations for action on measures that have a significant impact on the value of the transaction.

CRISIS MANAGEMENT – SECURITY IN DIFFICULT TIMES

Cyber insurance policies offer far more than financial protection: they ensure effective crisis management in order to respond quickly and effectively to security incidents. These include incident response procedures to detect, analyze and contain cyberattacks, legally compliant notifications and a business continuity plan (BCP) to secure critical processes. IT forensics, PR consultants and lawyers work around the clock on analysis, containment and recovery. Kessler assists with everything from reporting claims to coordinating with service providers and providing evidence to insurers.

CYBER RISKS AT SPIN-OFFS

In the event of a company spin-off, the seller often provides IT infrastructure on a transitional basis for 6 to 36 months and regulates this through a transition service agreement (TSA). Traditional cyber insurance does not cover this stage of the process: in the event of outages or attacks, there is a risk of substantial liability claims. One remedy to this is professional indemnity (PI) insurance, which covers errors or omissions in the provision of services and thus closes the coverage gap in IT transition scenarios.

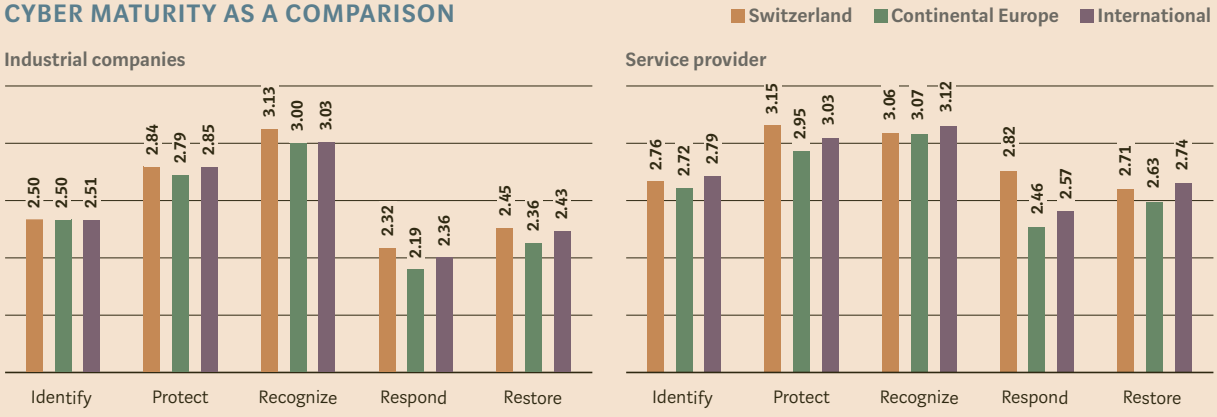
CYBER MATURITY AS A COMPARISON: WHERE DO SWISS COMPANIES STAND?

Since early 2024, Kessler has been using Marsh's Cyber Self-Assessment Tool (CSA), combined with the NIST Cybersecurity Framework, to assess the cyber resilience of clients (level 1 = partially implemented to level 4 = adaptive). Industrial companies in Switzerland score 2.71 on average, while service providers such as IT, finance and consulting firms score 2.91 – both of which are above the EU and international average. The lead held by service providers is particularly evident in the areas of "Protect" (+0.20) and "Respond" (+0.36). Rapid responses to incidents have proven to be critical with regard to damage mitigation.

SUPPLY CHAIN – INSIGHTS

IT service providers are of central importance to most companies, but at the same time they are a preferred target for attacks. Around a third of all cyber incidents can be traced back to them, primarily through incorrect configurations, unprotected accounts or delayed security updates. This is why every company should systematically include IT service providers in risk management, review them regularly and ensure cyber insurance also covers outsourcing incidents. While responsibility cannot be outsourced, risks can.

CYBER MATURITY AS A COMPARISON



The cyber insurance market

RANSOM NEGOTIATIONS

Extortion is a key element of the ransomware-as-a-service business model, with the aim being to release encrypted data or prevent its publication. Companies often pay the ransom out of a lack of alternatives. Cyber insurance sometimes covers ransom money as a last resort. Negotiations should ideally be conducted by specialist crisis advisers who manage communication and negotiations, check the credibility of the claims and attempt to reduce the ransom amount. The goal is to restore the data, ensure no new attacks will be mounted and disclose the attack method. They also make recommendations to prevent attacks in the future.

CYBERATTACKS IN 2024: MORE NOTIFICATIONS, FEWER CLAIMS

According to the Marsh Claims Report, claims notifications among cyber insurance customers in Europe increased by 61% in 2024. At the same time, growing resilience and faster responses to threats limit their impact. Driving factors included digital supply chain disruptions such as the global CrowdStrike outage. The proportion of ransomware cases fell from a peak of over 40% in 2021 to 18% in 2024, while AI-supported phishing attacks increased. It is worth noting that multi-factor authentication (MFA) remains the most commonly compromised security control.

ABOUT KESSLER

Kessler is the leading Swiss enterprise specializing in comprehensive risk, insurance and pension benefits consulting. We advise over 1,500 medium-sized and large Swiss companies from the service, trading and manufacturing industries, as well as the public sector. Thanks to our expertise in each of these economic sectors, our highly qualified staff and our leading market position, we contribute significantly to the long-term success of our clients. As a reliable partner, we inspire our clients and open up new perspectives through the safe and successful management of risks. Founded in 1915, Kessler has 370 employees working at its headquarters in Zurich and its other sites in Basel, Bern, Geneva, Lausanne, Lucerne, Neuchâtel, St. Gallen, Sion and Vaduz. As the Swiss partner of Marsh since 1998, we are part of a network with specialists in all areas of risk management and with great experience in handling global insurance programs. Marsh, the world's leading insurance broker and risk advisor, operates in more than 130 countries and is part of Marsh McLennan (NYSE: MMC).

Further information can be found at www.kessler.ch, www.marsh.com and www.mmc.com.

KESSLER & CO Inc.
Forchstrasse 95
P. O. Box
CH-8032 Zurich
T +41 44 387 87 11
www.kessler.ch

Marsh Network