KESSLER

Cyber Message 2026

Risk and Insurance



A SECURE FUTURE.

Cyber Message 2026

Cyber risk is about much more than just IT. Companies are increasingly being attacked through service providers, losses are blurring the lines between fraud and technology, and artificial intelligence (AI) is raising new liability questions. The way companies manage cyber risks has evolved over the years – from technical defense and prevention to preparing for when an incident actually occurs. Ten years of dealing with cyber risk at Kessler have shown: Things become particularly challenging where corporate governance, liability and insurance intersect, and where responsibilities, processes and coverage have not been clearly coordinated in advance.

Changes in the law

CYBER GOVERNANCE AS A MANAGEMENT RESPONSIBILITY

Cybersecurity is no longer just an IT responsibility. It has become a key management responsibility that is coming under increasing legal scrutiny. Boards of directors and executive management must consider cyber risks as part of their statutory duties of care and oversight. Cyber risks must therefore be firmly embedded in corporate governance, risk management and strategic decisions, such as outsourcing or M&A transactions. This requires clear responsibilities, regular reporting, appropriate oversight and a conscious approach to residual risks. Any potential transfer of cyber risks should also be reviewed, with decisions documented in a transparent and traceable way. If duties of care are breached and this results in a loss, members of governing bodies may be held personally liable. Directors' and officers' liability insurance (D&O) does not relieve them of their statutory obligations.

LIABILITY BETWEEN CONTRACTUAL COMMITMENTS AND CUSTOMER EXPECTATIONS

Today, customers expect more than just products and services that work. They also expect contractual assurances that digital components, data and systems are protected and will remain available. Providers increasingly find themselves pulled in different directions. The more specific the service-level agreements, the more likely they are to become the standard against which liability is assessed in the event of a dispute. Anyone who promises too much takes on risks that cannot be fully controlled from a technical or organizational perspective and that often have only limited insurance coverage. In practice, liability insurance generally covers statutory liability, but not additional liability assumed under a contract. Clear allocation of risk, realistic commitments and precisely defined limits of liability are therefore essential.

AI AS A RISK DRIVER

An AI agent accidentally deletes production data, a chatbot makes an incorrect commitment, or an AI tool processes personal data unlawfully: AI amplifies existing risks. It can accelerate cyberattacks, make phishing more convincing, facilitate data breaches, generate inaccurate outputs or trigger discrimination claims. Depending on the type of loss, different types of coverage may apply. Cyber insurance for security or data privacy incidents, professional liability for incorrect recommendations or technology services, crime insurance for fraudulently induced payments, and D&O insurance for matters involving oversight responsibilities. The key question is not whether AI itself is insured, but whether existing policies adequately cover the relevant risks associated with AI applications.

Current risks

TECHNOLOGY RISKS FOR INDUSTRIAL COMPANIES

Many industrial companies are now also technology companies. They develop software, offer digital platforms or enhance their machinery with IT services such as remote maintenance or software as a service.

This is making liability risks increasingly complex. The lines between product liability, professional liability and cyber insurance are becoming blurred. What might once have been machinery damage could now be a software failure, data privacy breach or purely financial loss. Traditional commercial and product liability solutions do not always provide adequate coverage for these risks. Industrial companies should therefore systematically assess their digital services and incorporate them into their risk management.

For companies operating across borders, the new EU Product Liability Directive adds to these liability risks: From December 9, 2026, software may be considered a product under certain conditions. Software defects or inadequate updates may give rise to product liability claims.

CYBERCRIME SCENARIO

"Please transfer CHF 500,000 immediately." The message appears to come from the CEO, and an employee makes the payment. But the instruction is fake – and the money is already gone. Which insurance covers the loss?

In our claims work, we see that these types of fraud can be technically sophisticated: a compromised email account, login credentials obtained via phishing, or an invoice containing altered bank details. For companies, the incident itself remains the same, but the way the loss is viewed from an insurance perspective can vary. Related costs such as forensics or recovery may be covered by cyber insurance, while a fraudulent transfer is more likely to fall under crime insurance – often subject to sublimits and verification requirements. Depending on the policy, the same incident may be fully or partially covered or not covered at all.

In this regard, the key is not just which policy is in place, but whether cybercrime scenarios have been thoroughly assessed. Relying on individual areas of coverage or failing to document processes can leave gaps despite apparently comprehensive coverage.

Cyber incidents

THE HIDDEN COST DRIVERS

Cyber incidents are expensive, but in our experience in Switzerland, this is rarely due to claims for damages. The legal hurdles are high – fault, causation and a specific financial loss must all be proven. In our cyber portfolio, claims for damages account for well under 5% of payments, including the cost of defending against unfounded claims. The real cost drivers are incident response, forensics, recovery, business interruption, reporting obligations and regulatory requirements – with financial, operational and reputational consequences.

For companies operating internationally, however, this does not tell the whole story. Liability risks vary depending on the jurisdiction: In the EU, companies may face fines and claims for damages under the GDPR, while in the US, class actions and punitive damages are a risk. What matters, therefore, is not only where the company is based, but also where its customers, subsidiaries or personal data are located.

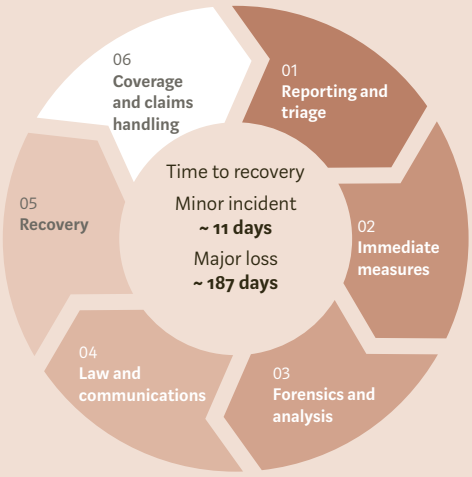
CYBERATTACKS ON IT SERVICE PROVIDERS

IT service providers play a vital role in keeping their customers' businesses running. When a provider is compromised, the impact often hits many customers at once – business interruption, data breaches and migration costs. The Unico Data case shows just how far-reaching the consequences can be. Following a ransomware attack in 2023, numerous customers were offline at the same time. At the end of 2025, the company ceased operations – not because of the immediate costs of more than CHF 1 million, but because of reputational damage and the loss of customers.

Who bears the cost of a loss like this? Contracts often limit claims to direct losses. Consequential losses and lost revenue are often only covered to a limited extent. If the service provider experiences an outage or goes out of business, contractual claims may ultimately be worthless. Its cyber insurance generally covers its own losses, not those of its customers.

Companies therefore need to make sure they have their own protection in place. Outsourcing agreements, liability limits, their own cyber insurance and business continuity plans should be reviewed regularly. After all, outsourcing IT services means handing over your systems – not your risk.

LIFE CYCLE OF A CYBER CLAIM



01 **Reporting and triage**
Assess the suspected incident, crisis response team
Tip: Report quickly and have a clearly defined crisis response team

02 **Immediate measures**
Isolate systems
Tip: Test the emergency response plan in advance

03 **Forensics and analysis**
Determine the cause and scope
Tip: Have clear contractual terms in place with the incident response provider

04 **Law and communications**
Meet reporting requirements
Tip: Check the threat group against OFAC sanctions before making payment

05 **Recovery**
Systems, loss of income
Tip: Do not attempt recovery yourself, to ensure evidence is preserved

06 **Coverage and claims handling**
Documentation, settlement
Tip: Keep complete records from the very beginning

The cyber insurance market: 10 years of cyber expertise at Kessler

Since Kessler placed its first cyber insurance policy in 2016, the market has changed significantly. From 2020, market conditions tightened, with high losses, limited capacity and increasing cybersecurity requirements. It has eased since then. Additional capacity and stronger competition have created new opportunities for placing coverage. At the same time, AI-enabled attacks, supply chain risks and increasing regulation are making the landscape more challenging. Strong security standards, clear risk information and effective loss prevention remain key to insurability.

Today, our specialized cyber team provides comprehensive support, working with our partner Marsh where needed – from self-assessments and maturity analyses through to claims support. We have also developed a framework agreement solution for small and medium-sized companies, tailored to their needs and offering attractive terms. In 2026, we placed Cyber blue line for another three years. Our commitment remains the same: identify risks early, strengthen resilience and provide reliable support to our clients when an incident occurs.

ABOUT KESSLER

Kessler is the leading Swiss enterprise specializing in comprehensive risk, insurance and pension benefits consulting. We advise over 1,600 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 390 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 is a global leader in risk, reinsurance and capital, people and investments, and management consulting, with more than 90,000 colleagues advising clients in 130 countries (NYSE: MRSH).

For more information, visit www.kessler.ch, www.marsh.com and www.corporate.marsh.com.

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

MARSH Network