KESSLER

Cyber Message 2024

Risk and Insurance

A SECURE FUTURE.

Companies are facing an increasingly complex landscape of cyber threats nowadays. In addition to the already known forms of attack, it's becoming clear just how dependent we are on external service providers in particular. Read the second edition of the Kessler Cyber Message to learn how the general cyber market has developed over the past year, the role that people play within a company and how we optimize our risk assessment process.

Changes to the law

nFADP

The rapid pace of technological progress means it is vital to continuously update legislation. The new Swiss Federal Act on Data Protection (nFADP), which brings Switzerland's data protection provisions more in line with those set out in the EU's General Data Protection Regulation (GDPR), entered into force on September 1, 2023. The law has been revised to improve personal data protection.

The main reforms include more extensive access, reporting and information obligations. Companies have to provide data subjects with comprehensive information on their data collection and processing activities, and report any data breaches to the Federal Data Protection and Information Commissioner (FDPIC). The FDPIC has received more than 200 reports from various sectors to date. The nFADP introduces greater responsibility, a need for companies to make adjustments, higher compliance costs and potential changes to business practices.

On August 14, 2024, a new Swiss-US Data Privacy Framework was enacted to enable secure exchange of data between Switzerland and certified companies in the US – without any need for additional safeguards. The purpose of this new framework is to ensure that data protection measures are actually implemented. An official list of all certified companies can be found at https://www.dataprivacyframework.gov/list.

LAWFULNESS OF RANSOMWARE PAYMENTS

While the Swiss Federal Council and other governments are looking for effective ways to deal with the problem of ransomware, the legal framework already offers relevant regulations. Even without a specific ban, there are significant legal risks for organizations that pay ransoms. Such payments could violate Article 260ter (1) (b) of the Swiss Criminal Code, for example, if they are made to criminal organizations.

It is therefore essential that decisions to pay ransoms are made carefully and in a well-founded manner In Switzerland, the law has so far been applied in practice in a way that favors the victims. Companies that have taken matters into their own hands by paying ransoms have not yet faced additional penalties from the authorities.

ARTIFICIAL INTELLIGENCE

The threats that AI-generated attacks pose are still a very current topic of conversation. The EU AI Act entering into force on August 1, 2024, underscores the need for greater regulatory protection. The EU developed the AI Act to safeguard ethical values and fundamental rights, and its purpose is to provide a secure environment for users and businesses alike.

Current risks

THE HUMAN FACTOR

Cyber criminals often target employees to get around companies' security measures and penetrate their IT systems, which can cause significant damage. Employee behavior has a direct impact on cybersecurity, not to mention on mitigating the impact of an attack. Protection and damage limitation are key aspects of cyber resilience.

The latest research has shown that employees' attitudes towards cyber risks are crucially important. If employees understand that they are working with sensitive data on a daily basis, this raises their awareness and improves security. It is vital to highlight the influence that each individual has on cyber resilience. Concrete examples, sector-specific references and regular training programs promote long-lasting awareness and foster a security-focused mindset.

PROFESSIONAL LIABILITY RISKS FOR TECH FIRMS

Tech companies rely heavily on complex IT systems, while the technical risks are constantly increasing at the same time. Depending on the type of company and the services it offers, this can lead to severe consequences. Breaches of duty, omissions, system outages and software bugs can result in significant problems and liability claims. Professional indemnity insurance (PI) is therefore a meaningful option to protect companies against professional risks.

Tech firms that are more exposed to external attacks face a greater risk of cyber incidents. While PI tech insurance covers the risks associated with errors or omissions when providing services or with technical products, cyber insurance covers external threats such as hacker attacks, data leaks or business interruptions. By taking out both types of insurance, tech firms can rest assured that they are comprehensively covered.

The cyber insurance market

MARKET UPDATE

The cyber insurance market has been dynamic and highly competitive since the end of 2023. It is increasingly being invigorated by new insurers. The trend is still moving toward more flexible underwriting guidelines, higher insured sums and, often, also reduced premiums for the same scope of cover. At the same time, strict minimum requirements for the policyholders' IT maturity, such as the "12 Key Controls", remain a constant. These requirements are crucially important when it comes to taking out cyber insurance. The development of the market shows that Swiss insurers are becoming more open to risk, while at the same time seeking to strike a balance between caution and innovation.

GENERAL DEVELOPMENT IN THE CLAIMS ENVIRONMENT

Ransomware attacks are still the biggest risk and cause the most substantial financial losses. Companies often underestimate the many different elements of the damages they might suffer. The costs of crisis management, system recovery and the impact of a business interruption can quickly rise sharply.

Ransom demands are still a serious problem. In the event of extortion, it is advisable to enter into negotiations to gather information and play for time. Kessler's statistics show that this reduces median ransom demands by 59%.

BUSINESS INTERRUPTIONS DUE TO CYBER INCIDENTS

Calculating revenue loss after cyber incidents is challenging, as it is influenced by seasonal and economic fluctuations. The revenue figures have to be compared with the budgeted amounts and the figures of the previous year. Solutions such as business impact analyses are both time-consuming and expensive. Documenting additional costs is problematic too. Kessler recommends keeping records of overtime and additional measures to improve verifiability and crisis management. In addition to the hours staff work, the activities they carry out during this time should be recorded as well, so that they can be tracked at a later date.

THE CROWDSTRIKE INCIDENT

The CrowdStrike incident in July 2024 illustrated just how critical a faulty third-party update can be. A bug in the Falcon content update triggered global outages for Windows users. An event like this can jeopardize the integrity of the entire supply chain, which is why suppliers shouldn't only be assessed once, but rather continuously as part of an ongoing process. Clear security standards and regular audits are essential in contracts with third-party providers. Such measures help to protect the integrity of data and minimize the impact of such incidents.

CYBER SELF-ASSESSMENT (CSA) TOOL

Since early 2024, Kessler has offered its clients the Cyber Self-Assessment (CSA) tool provided by its network partner Marsh. The web-based questionnaire makes it easier to record information relating to risks, and the questions are tailored to the size of the company and its activities. The ability to reuse data for subsequent years, and broad acceptance among insurers, greatly simplify the call for tenders and renewal process.

But that's not all that the CSA offers. It generates reports on insurers' assessment of a company's IT maturity, indicates how controls are to be classified in comparison to international frameworks and shows how the company is positioned in a peer benchmark. In addition, the Blue[i] analysis tool models potential loss scenarios, including probabilities of occurrence and expected extent of loss. These insights support the risk transfer evaluation and refine the tendering strategy. They indicate what measures can be taken to make targeted improvements to an organization's cybersecurity.

CYBER BLUE LINE

The introduction of cyber blue line in 2023 has been a resounding success. Cyber blue line significantly simplifies the cyber submission process. If the 12 minimum requirements are met, more than 98 % of our clients decide to switch to cyber blue line. Under the framework agreement, our clients also benefit from services such as phishing simulations and staff training.

THREEMA

To ensure secure communication even in a crisis, we rely on our collaboration with Threema. In 2024, the market research company Forrester recognized Threema as a leading provider of secure communications. Companies often fail to verify how they would communicate in a crisis. Our clients are grateful to have their attention drawn to this fact and make use of the secure communication channel via Threema offers.

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 350 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