KESSLER

Cyber Message 2023

Risk and Insurance

A SECURE FUTURE.

Companies are more vulnerable than ever to cyber attacks. For most, cyber incidents rank among the top three business risks. But the rise in cases is affecting insurers just as much as the companies themselves. In this Cyber Message, we share our experiences and lessons learned from various incidents.

Legislative changes

NEW DATA PROTECTION ACT

The new Federal Act on Data Protection (nFADP) came into force on September 1, 2023. But why was it necessary to change the existing law? The original law was introduced back in 1992. Much has changed in 31 years, particularly as we have entered the digital age. To protect the privacy of every individual, it is essential to update the data protection laws in line with developments. The correlation between information security and data security can be seen in the main security objectives of confidentiality, integrity and availability.

What are the main changes?
- The new law covers personal data, but no longer extends to the data of legal entities
- New documentation obligations
- Strengthened rights of data subjects
- Introduction of the principles of "privacy by design" and "privacy by default"
- Criminal liability of the responsible person

There was no transition period for the new law. What do we recommend to our clients? Simply to ensure that all responsibilities are clearly allocated and that those responsible are aware of the requirements.

REPORTING OBLIGATION FOR CRITICAL INFRASTRUCTURE

A further regulatory change will take the form of a revision of the Information Security Act (ISA), which defines new standards for federal authorities and organizations in particular. These standards are aimed at improving information security and cyber security. For example, all affected authorities and organizations are required to establish an Information Security Management System (ISMS) and have adequate risk management measures in place.

In addition, organizations in critical infrastructure sectors are obliged to report serious cyber incidents to the National Cyber Security Centre (NCSC) within 24 hours of discovery. Failure to comply with this reporting obligation may result in a fine of up to CHF 100,000.

Critical infrastructure includes universities, public authorities, security and rescue organizations, drinking water and wastewater plants, waste management companies, energy providers, banks, insurance companies, healthcare facilities, social security institutions and the Swiss Broadcasting Corporation. The new legislation is expected to come into force shortly.

Current risks

EVOLUTION OF RANSOMWARE

Ransomware remains one of the biggest risks for most clients. SMEs in particular are becoming increasingly attractive targets for cyber criminals. Small and medium-sized businesses usually do not invest as heavily in IT security as larger corporations. In general, it appears that ransomware attacks are becoming less industry-specific. There has been a noticeable increase in attacks since mid-2022.

It is interesting to note that the attackers' modus operandi has changed in some cases. Because companies have invested more in detection and response, many hacker groups have shifted their focus from data encryption to exfiltration and the threat of publication. Some groups even contact the targeted companies after a successful attack and try to find out their coverage under their cyber insurance policies.

In such cases, cooperation with the attackers without the prior consent of the insurer is strongly discouraged. Any form of cooperation constitutes a breach of the insurance terms and may affect a payout in the event of a claim.

ATTACKS ASSISTED BY ARTIFICIAL INTELLIGENCE (AI)

With the rapid development of AI, the possibilities for digital fraud have also greatly expanded. This is particularly evident in the latest methods used for phishing emails and what is known as social engineering fraud (SEF). Furthermore, advances in deepfake technology now allow fraudsters to manipulate audio and video recordings convincingly enough to persuade victims to transfer money or reveal information on virtual meeting platforms. The criminals often impersonate senior executives to induce employees to engage in these activities.

Similarly, the platform WormGPT enables creation of large volumes of sophisticated emails for use in phishing attacks, including business email compromise (BEC). It should be noted that traditional SEF, which does not involve manipulation of the insured's computer systems, will usually be covered under crime insurance rather than cyber insurance.

Insurers in the Cyber Market

12 KEY CONTROLS

The minimum requirements for obtaining cyber insurance can be broken down into 12 key controls. According to a study by our network partner Marsh, compliance with these controls has a significant influence on loss prevention. However, the effectiveness of the individual key controls varies considerably.

A comparison of the minimum requirements with the loss database showed that hardening techniques in particular reduce the probability of a successful cyber attack. Hardening techniques are those security precautions and configurations put in place to make systems, networks and software more resilient to potential threats and attack.

So far, most insurers have focused their attention on the key controls of multi-factor authentication (MFA), endpoint detection and response (EDR) and privileged access management (PAM). The study also found that MFA has a strong positive impact only when fully implemented.

BREACHES OF OBLIGATION

Policyholders have numerous obligations under the general terms and conditions of their policies – and this is also increasingly the case in the cyber insurance market. These range from implementation of appropriate technical safeguards and procedures to professional verification of the adequacy of their computer systems and IT processes. The goal is to maintain the integrity, availability and confidentiality of the data stored on these systems.

In the event of a culpable breach of these obligations by the policyholder, the insurer may reduce the amount paid out in the event of a claim. The burden of proof for such a breach lies with the insurer. The policyholder would not be penalized if the breach of obligation is considered non-culpable under the circumstances or had no influence on the occurrence of the insured event or the scope of cover provided by the insurer (since the revision of the Insurance Policies Act). This revision represents an improvement of the legal position of the policyholder.

Cyber insurance market

MARKET UPDATE

The cyber insurance market continues to stabilize in 2023. Insurers are generally able to maintain capacity and level of cover. Premiums have risen by less than 10 percent on average, marking a huge improvement compared with previous years.

For particularly exposed clients, such as hospitals and service providers in critical infrastructure sectors, larger adjustments were necessary in some cases. The conclusion of a cyber insurance policy should be understood as a quality indicator of a high level of cyber security maturity. Implementation of the 12 key controls is therefore consistently demanded. And it is having an effect: Although there has been a significant increase in cyber incidents worldwide since mid-2022, primarily ransomware attacks, the number of incidents reported by Kessler and Marsh has decreased over the same period.

KESSLER BLUE LINE FACILITY

To make the process of submission of a cyber insurance policy more efficient, we have developed a solution. Our Kessler blue line Facility enables small and medium-sized companies to take a new approach. Provided a company is eligible, we dispense with the annual renewal process, and the company benefits from an exclusively negotiated contract at a competitive premium.

CYBER ATTACK? SECURE COMMUNICATION WITH THREEMA

In the cyber world, crisis communication is and will continue to be crucial. However, many organizations – whether large corporations or SMEs – lack a secure platform for communicating quickly and effectively with key personnel and members of their crisis management team in the event of a crisis.

Recognizing this gap, Kessler teamed up with Threema to develop a solution for dealing with a potential crisis. From January 1, 2024, our cyber insurance will include free access to the Threema Work communication app for our clients' crisis management teams. We are thus offering our clients a secure platform for communicating smoothly in the event of a crisis.

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 330 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