CORPORATE
CYBER INSURANCE

For a rainy day

Prager Dreifuss lawyers explain how companies and banks can best protect themselves from the threat of cyberattacks

1 MINUTE READ

With digitalisation becoming ever more prevalent in everyday life and the internet of things on the horizon, it has become evident that with increasing electronic efficacy and ease comes a greater and more demanding risk assessment for a whole range of new threats to companies embracing such technologies. Reto Jenny and Christian Casanova of Prager Dreifuss' insurance and reinsurance team discuss the new challenges posed by cyber risks and how companies may best prepare against potential onslaughts on the insurance front.

The awareness of cyber risk has significantly increased recently, partly because of the the General Data Protection Regulation (GDPR) coming into force, and wide-spread media coverage of recent cyberattacks such as the encryption trojan NotPetya and ransomware cryptoworm, WannaCry. Estimated global costs associated with these cyberattacks are significant:$300 million for NotPetya and up to $4 billion for WannaCry. Some cyberattacks were specifically aimed at Swiss companies, with one targetting a Swiss telecom provider and its service providerresulting in the addresses of some 800,000 customers of the provider being stolen.

The financial aspect of cyberattacks is estimated to cause annual losses of $600 billion worldwide and CHF 9.5 billion for Switzerland.

The increased awareness of cyber risk is corroborated by a recent survey of a leading Swiss broker, showing that 79% of the companies it interviewed qualified cyber issues as a top 10 risk. The importance of dealing adequately with cyber risk is also demonstrated by recent action by the Swiss government. In 2018, the Swiss Federal Council adopted the new national strategy for the protection of Switzerland against cyber risk. Also, the Swiss Federal Office for National Economic Supply issued a minimum standard for improving ICT resilience which serves as a recommendation, in particular for operators of critical infrastructure, but also for any business or organisation, as well as an ICT minimum standard assessment tool. Similarly, cyber risk is also part of the focus of the Swiss Financial Market Supervisory Authority.

The consequences of a cyberattack can be manifold and their financial impact on a company can be critical. Consequently, it seems to be well within a board director's duty to at least examine whether a cyber-insurance policy should be taken out. Included in the statutory non-transferable directors' duties is a duty to establish a risk management (cf. article 716a(1)(1) of the Swiss Code of Obligations, CO). Failure to carry out cyber-risk management at all, or to carry it out properly, may qualify as a breach of care and duty (article 717 CO) and potentially result in D&O claims (article 754 CO).

What are cyber risks?

Cyber risk, cyber losses or damage and cyberattacks are not fixed legal terms nor is there a clearly defined general understanding based on language usage. While there is no established interpretation of cyber risks, an often quoted definition understands cyber risk as "*operational risks to information and technology assets that have consequences affecting the confidentiality, availability, or integrity of information or information systems*" (Cebula, Popeck and Young, A Taxonomy of Operational Cyber Security Risks Version 2, May 2014, p. 1). The European insurance and occupational pensions authority EIOPA understands cyber risk as "*any risks that emanate from the use of electronic data and its transmission, including technology tools such as the internet and telecommunications networks. It also encompasses physical damage that can be caused by cyberattacks, fraud committed by misuse of data, any liability arising from data storage, and the availability, integrity and confidentiality of electronic information – be it related to individuals, companies, or governments.*"

In a wide sense, cyber risk is connected with the technology and information of a given company. Typical examples include forms of cyberterrorism, cyber criminality (including extortion), identity theft, the spying on, disclosure and/or theft of sensitive information (addresses, credit card information, passwords, etc.), business interruption resulting from a hacking attack, damage to data by a hacker, so-called Distributed Denial of Service Attacks (DDoS), whereby typically a server of a company is flooded with superfluous requests to overload systems and thereby paralyse the server, and the introduction of malware (viruses, worms and other malicious codes) into a firm's IT system.

The resulting loss can take various forms, including data loss or corruption (including recovery costs), privacy breaches (including fines and legal costs), damage to reputation, ransom payments in case of cyber extortion, loss of earnings due to business interruption and the cost of experts and advisers. In other words, losses as a consequence of materialised cyber risks may include first-party losses such as business interruption, ransom payments, cyber theft, data restoration, etc. as well as liability claims of third parties against the company such as data protection liability (including fines).

The source of the cyber risks can be within or outside a company, such as an external hacker attack, or data theft by an employee. From a company's perspective, the thorough analysis of potential cyber risk is essential for taking out a cyber policy as the market does not typically offer an all-encompassing policy that insures against all sorts of cyber risk (no all-risk policy) but rather only offers policies covering certain risks.

Possible coverage of cyber risk under conventional policies

The question arises if, and to what extent, such cyber risks may be covered under conventional policies, such as property insurance, liability insurance, D&O insurance, and fidelity insurance. This issue has recently drawn the attention of regulators, triggering warnings of insurance companies' exposure to "silent" cyber risks sitting in their portfolios of conventional policies. Insurers have now started addressing the cyber risks in traditional P&C policies by way of exclusions. In any event, in every single case, an analysis of possibly applicable policies and their general conditions of coverage is required. For the purpose of this article, we have analysed selected Swiss "conventional" as well as cyber policies. The following comments are therefore not to be understood as being applicable for all policies. An analysis of potential coverage will always have to rely on the specific circumstances of the case as well as the possibly applicable policies in that case.

Liability insurance is not suitable to protect the insured against all possible losses due to the realisation of a cyber risk

Property insurance

Typically, a property insurance requires property damage, i.e. the damage, destruction or loss of a (physical) object. With regard to electronic insurances where the insured object includes a data carrier, the question may arise whether data itself could constitute an object in the legal sense. This could of course only be an issue where the policy does not explicitly mention that data itself is not an insured object (cf. the non-binding sample conditions of the Swiss Insurance Association for electronic data processing equipment that clarify that data and software are not insured and costs related to the recovery of data may only be covered if an extension is agreed upon). While a minority of Swiss legal scholars is of the view that digital data may constitute an object in the sense of the Swiss civil code, most Swiss legal scholars do not share this opinion on the basis that data is not a physical object.

Cyberattacks, however, often do not amount to damage, destruction or loss of a (physical) object, i.e. to property damage. In addition, even where an extension for costs related to the recovery of data is agreed upon, coverage requires, as matter of principle, the damage, destruction or loss (by theft) of a data carrier, and data modification or losses owing to viruses, trojans and worms are typically excluded from coverage. Furthermore, property insurance only covers first party losses, but no liability claims.

Liability insurance

Liability insurance protects the assets of the insured by covering liability claims that are validly raised against the insured and by covering the costs of defending liability claims. As far as business liability insurance is concerned, it typically only covers property damage and personal injury, or consequential financial losses flowing from such property damage or personal injury, but not so-called pure financial losses (a financial loss which can neither be qualified as property damage nor personal injury). As a matter of principle, the mere functional impairment of an object without impairment of its substance does not qualify as property damage.

Professional liability insurance for IT service providers typically covers claims for damages asserted against the insured persons on the basis of statutory liability provisions for personal injury, property damage and financial loss. The policy would define which types of liability claims are covered, and typically includes claims for damage caused or partly caused by the intrusion of malware (such as viruses, trojans, etc.) as well as by unauthorised access by third parties to data or IT systems.

In some policies, there is the explicit coverage requirement that the policyholder be able to prove the implementation of customary and up-to-date protection systems (such as antivirus software and firewalls). Also, there are a number of exclusions that may make it difficult for insured persons to obtain coverage, such as exclusion with regard to the insured's product, work or services not corresponding to the state of the art, or in case of the violation of recognised rules of software engineering.

Furthermore, it does not cover first-party losses. Liability insurance is not suitable to protect the insured against all possible losses due to the realisation of a cyber risk; for example, against the costs for the recovery of lost data.

Fidelity insurance

Fidelity insurance, as a matter of principle, covers financial losses of the insured that are intentionally caused by employees or third parties. Under fidelity insurance, direct losses incurred by an insured company resulting from hacker attacks may be covered which are the result of intentional, unlawful and targeted intrusions by third parties in the IT system of the insured company, provided that the third party was enriched in the amount of the damages and to the extent that the third party is liable.

However, such coverage would typically need a 'targeted' hacker attack, i.e. an attack directed against a defined number of IT users. This requirement may in many cases exclude an indemnification of the insured. Depending on the terms of the policy, there may also be explicit coverage for certain indirect damages such as expenses for the continuation of business operations (over a certain period) and for money transfers after misuse of users' access data. Furthermore, coverage for the costs of mitigation measures regarding reputational damage, as well as damage investigation and prosecution costs, may be granted. Conversely, other indirect damage such as a loss of earnings due to business interruption is not covered.

As will be seen later, there may be a certain overlap between a fidelity and a cyber risk policy. However, many losses due to cyberattacks are not covered under a fidelity insurance. For example, all losses which were caused by negligence or a loss of earnings due to business interruption.

D&O insurance

D&O insurance typically contains no exclusions for cyber risks. While D&O insurance covers liability claims against directors and officers, cyberattacks will rarely result from the actions of directors and officers, but ordinarily have their origin outside the company. Also, in many instances, a director or officer will not be liable (through omission) for losses due to a cyberattack. However, the failure to analyse whether a cyber insurance must be taken out or not may trigger D&O claims.

Cyber insurance policies provide certain protection against these risks, but their scope is not uniform

Coverage under Cyber policies

Insured risks and benefits/losses

Which risks and losses are insured under a cyber risk policy depends on the respective policy and its general conditions of insurance, in particular the respective definition of the insured risk and covered losses. According to a 2017 study of the European Union Agency for Network and Information Security (ENISA) the lack of commonality in risk assessment language is a difficulty for the cyber insurance industry. Unlike insurance associations in other countries, the Swiss Insurance Association has not provided model general terms of coverage for cyber risks in Switzerland.

Typically a cyber policy covers certain first-party losses and certain third-party losses (liability claims) and also grants further benefits. As to coverage components, according to the 2017 ENISA study, first-party loss coverage may include network interruptions such as loss of business income due to cyber incidents, cyber extortion, electronic data incidents, cyber theft, data restoration, system clean-up costs, administrative investigation and penalties. Coverage for third-party loss may include data protection and cyber liability, media liability, the wrongful collection of information, media content infringement/defamatory content, and violations of notification obligations. Other, and important, benefits include, for instance, first response: crisis management, IT experts, breach-related legal advice, etc. What can be seen from that study, and what, in some cases, was reflected in the reviewed Swiss policies, is the approach of providing some basic cover against cyber risk, with the option of buying additional cover through extensions, such as for example, cyber extortion.

The reviewed Swiss policies contain coverage components for liability claims, a firm's own losses of a party, data protection proceedings and crisis management. As seen above, there is no commonality in the risk assessment language, including policy language. In an effort to identify some common features in the comments below, there was the need for some simplification. The exact scope of coverage will therefore always depend on the language of the respective policy.

Liability claims

Liability claims for data protection violations, or confidentiality violations, were covered in all the reviewed policies. The liability claims are, as regards the temporal scope of the policy, covered on a 'claims made' basis, i.e. the policy is triggered if the claim is first made during the policy period. Data protection violations are sometimes broadly defined as a violation of applicable data protection provisions, such as the Swiss Federal Act on Data Protection and of any comparable Swiss or foreign legal provision. Other policies appear to have a slightly narrower scope as they rely on the occurrence of a data protection incident, such as the loss, theft or unauthorised disclosure of personal data or data of companies that is not publicly available.

The reviewed policies also grant coverage for legal liability claims resulting from a violation of the network security, for example the theft, alteration or deletion of electronic data on the IT system of the insured or the unauthorised access to, or use of, the IT

There remains an essential but challenging task for companies to analyse which risks need to be covered

system of the insured. Legal liability claims due to DDoS attacks by the insured on third parties (as the result of the unauthorised access to the IT systems of the insured) are insured according to one policy, while other policies would typically only cover legal liability claims against the insured due to DDoS attacks on the insured's IT system. For example, if the insured cannot provide services because of the DDoS attack.

Furthermore, some policies do not only cover liability claims, but also defence costs for administrative proceedings in relation to data protection or confidentiality violations. Sometimes, it is explicitly provided for, in that the defence costs for internal investigation of an insured party in connection with such data protection or confidentiality violations are covered. Additionally, according to the policy language, administrative penalties and fines may also be covered under the condition that such penalties and fines are insurable according to the applicable legal system. This reflects the somewhat unclear legal situation: under Swiss law it is questionable, as a matter of principle, whether criminal fines are insurable.

Some policies provide explicit coverage for liability for the insured's electronic publications resulting from plagiarism, violations of personality rights of third persons, intellectual property rights, libel, unauthorised use of titles, formats, plots, etc. Also, depending on the policy language, claims or contractual penalties of the Payment Card Industry Security Standards Council, an acquiring bank or other institutions due to data protection or confidentiality violations may be covered.

First-party losses

Cyber policies also provide insurance cover for a number of defined first-party losses, such as a loss of earnings due to damage to reputation, crisis management costs, data recovery and system improvement costs, cyber extortion payments and financial losses incurred as a direct consequence of a cyberattack such as erroneous payments to third parties.

Again the scope of cover will depend on the respective terms and conditions of the relevant policy. As to the temporal allocation, the policies typically rely on the moment when the damage (non-availability of IT systems for business interruption) is first noticed. Other policies rely on the occurrence of the damage, and only – if that moment is not ascertainable – on the moment when the damage is first noticed.

Exclusions

Typically, cyber policies contain a number of specific exclusions which are known from 'traditional' policies, such as losses in connection with actual or alleged violations of antitrust law, contractual liability in excess of a legal liability (with certain carve-backs) claims for the fulfillment or not proper fulfillment of contractual obligations (with certain carve-backs), (certain) intellectual property violations, terrorism and war, etc.

Owing to advancing digitalisation, for example the internet of things, risks faced by companies due to cyberattacks will undoubtedly increase. Traditional policies will not provide sufficient protection against such risks. Cyber insurance policies provide certain protection against these risks, but their scope is not uniform. In this regard, the situation in Switzerland does not differ from the situation in other jurisdictions, and it remains to be seen whether some general standard for coverage will emerge once more experiences have been made with cyber insurance policies. Having said this, cyber policies include many elements which are also common in traditional policies, and it appears that the analysis of cyber insurances can in many aspects, rely on established practice for these elements. There remains an essential but challenging task for companies to analyse which risks need to be covered, and to what extent, in order to have suitable cover in place.

Reto Jenny
Partner
Prager Dreifuss, Zurich

Christian Casanova
Partner
Prager Dreifuss, Zurich