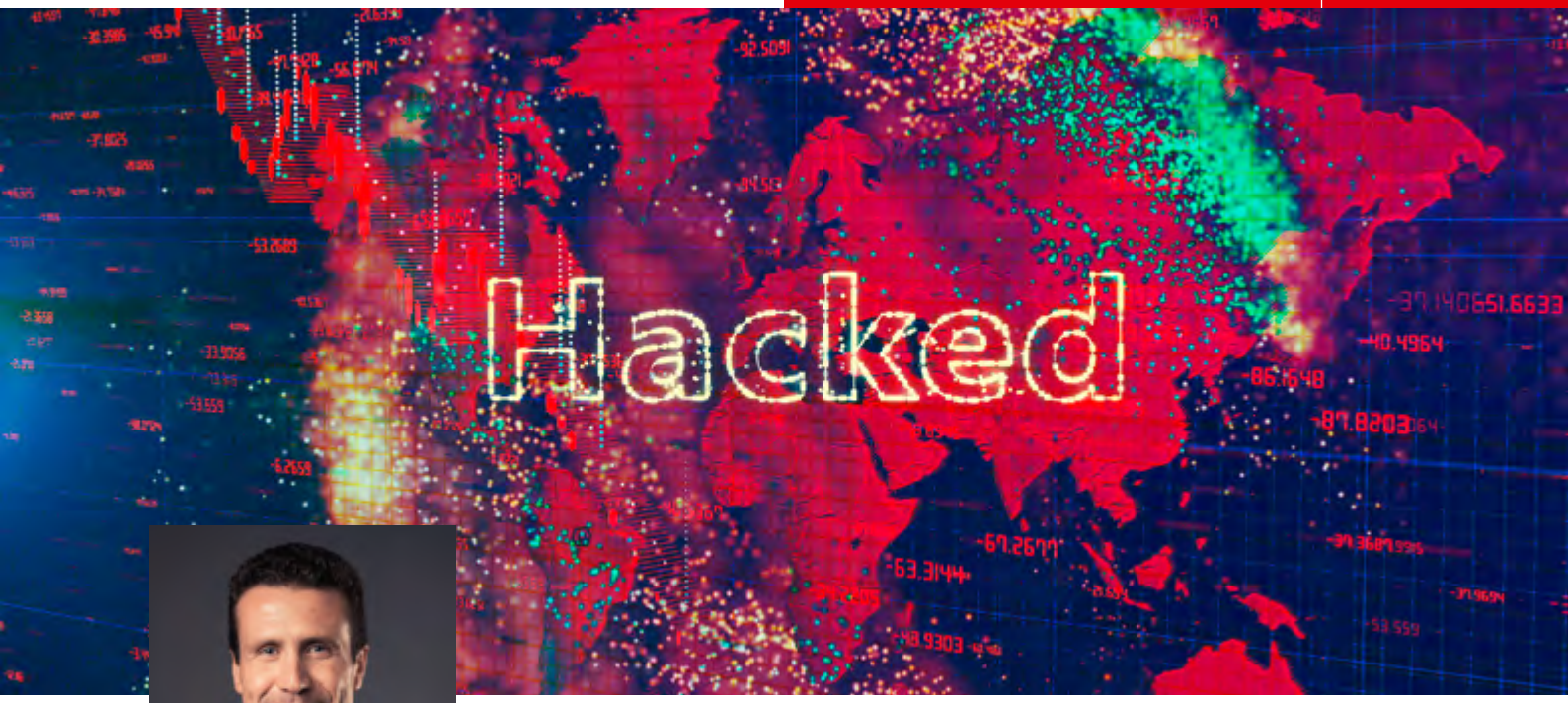
SWISS RISK & CARE
Our independence ▪ Your best insurance

INSURANCE INSIDE

N° 25
MARCH 2022






# EDITORIAL

## Cyber threat, a major risk about which still too little is known

Will 2022 be the year the pandemic ends? At a time when, like several countries in Europe, the Federal Council is lifting measures to combat the virus, there is hope of a return to normality. Let's hope for our businesses as well as for our personal lives that this return will be long term.

While the health crisis is receding, cyber threat, however, continues to grow. The war that has just broken out in Ukraine is also digital and involves an increase in cyber attacks. There is henceforth an ever-growing fear of a digital pandemic, i.e. the simultaneous attack of several companies in several places on earth with the aim of paralysing the world economy.

All companies are affected regardless of sector. Large companies and multinationals have realised that cyber risk is not just a matter for the IT department but is now an absolute emergency that is the responsibility of management and the board of directors. Conversely, all too often, SMEs underestimate their risk exposure and fail to invest sufficiently in their security. Less well equipped to prevent the risk and also to respond quickly and effectively to an attack, they find themselves increasingly frequent targets of hackers. Sometimes with dramatic consequences on their business.

Under these circumstances, is cyber insurance a solution? Yes, it undoubtedly is, but it is still necessary to understand what such policy covers and the conditions under which the policy may be taken out. This is what we would like to show you over the next few pages.

I would like to take this opportunity to share with you how proud I am to be the new CEO of Swiss Risk & Care. I would like to continue the work we have been doing for several years, which has prioritised investing in digitalization and IT security to strengthen our service and proximity to our client.

We hope you enjoy reading this paper!

**David Cochet**
Chief Executive Officer

SWISS RISK & CARE
Our Independence • Your best Insurance

# What is cyber insurance and should I underwrite an insurance policy?

**Not a day goes by without a company, large or small, falling victim to a cyber attack. For organisations, it's no longer a matter of if but when they will fall victim. Faced with this situation, how do insurers cover the risk? Review of the current situation.**

Cyber insurance is the ultimate solution once the company has implemented all the preventive measures to protect its digital data, secure its IT environment and comply with the regulations in force. *"Without doing this work beforehand and making the necessary investments as a result, it will be difficult for a business to take out insurance",* explains Sophie Di Meglio, Director of Special Risks at Swiss Risk & Care.

## What cyber insurance covers

Cyber insurance will apply in the event of a security incident or attacks on a company's IT system, or personal and confidential data. It mainly offers:

- **Assistance and crisis management:** the insurer provides the company with a 24/7 hotline to connect it with IT specialists, crisis management experts and legal advisors. This service can be mobilized during the first hours of an attack and is crucial in managing the crisis in order to mitigate its impact, especially on the company's reputation.
- **The first party cover:** covers, in particular, the costs incurred to restore data, remove malware, and notify the authorities and third parties, monitoring and surveillance costs as well as loss of income following the disruption of business (with a deferred period of between 6 and 48 hours depending on the insurer). Costs related to cyber extortion, such as the cost of consultants mobilised to prevent the threat of blocking or data theft from being carried out are also covered. Some insurers even agree to pay the ransom if there is no other alternative, but this is becoming increasingly rare. In the event of an incident, this guarantee should extend to the policyholder's service providers who manage its IT system or host its data.
- **Civil liability cover:** covers the costs of defence and damages, if any, in relation to third-party claims related to data protection, or in the event of infringement in relation to electronic content distribution.

Some insurers offer a cyber extension to their Property insurance policy and/or to their Liability insurance policy, but the coverage is generally less, and the financial compensation is low. *"Nevertheless, it is an interesting solution for SMEs,"*

> *"Insurers' criteria and terms evolve over time, in particular owing to the exponential increase in the number of cyber attacks over the past 2 years."*

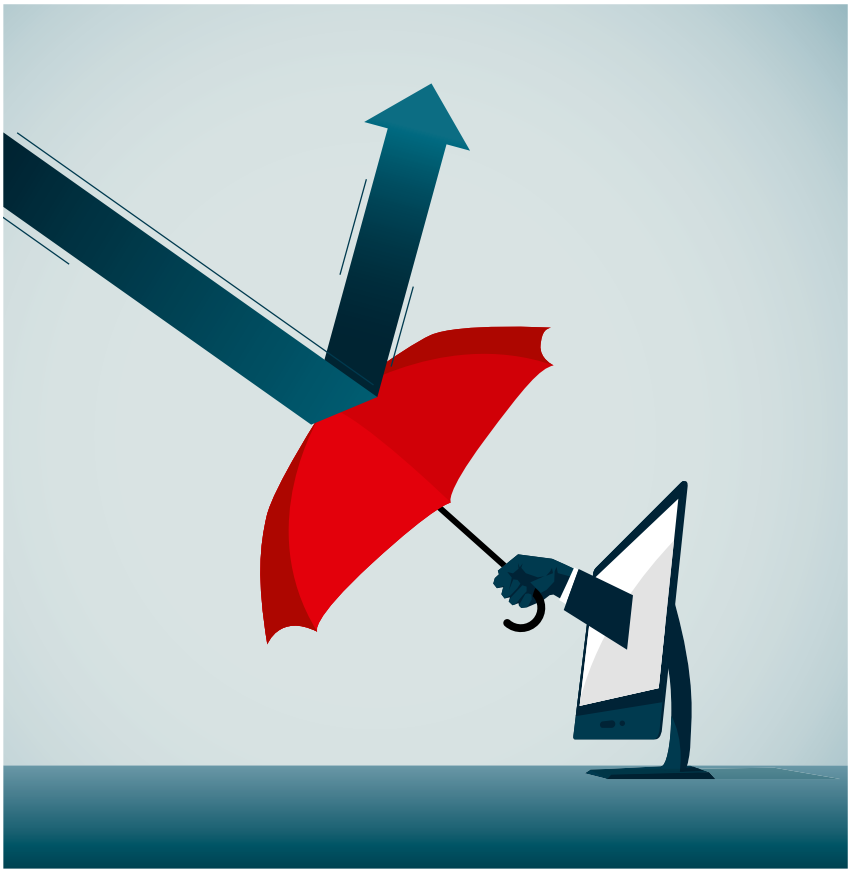
## Key figures

**1 attack every 39 seconds**

**USD 6,000 billion**
estimated **for the cost of attacks** (which is higher than the GDP of Japan) **in 2021**

**+ 400%**
**more attacks in 2020**

**more than USD 1,000 billion**
**spent on cybersecurity in 2021**



says Sophie Di Meglio, *"as the companies that pioneered Cyber insurance are now more demanding before insuring them, and some even no longer insure SMEs with turnover below a certain level."*

## And what it does not cover

Among the main exclusions, we have personal injury, harm to property and financial loss other than harm to property, loss due to wear and tear, or ageing of data carriers, or the lack of compatibility between digital data and software, or between software programmes, the failure or breakdown of public utility infrastructures (network disruption), the infringement of commercial patents, etc. The obligations imposed on the policyholder differ from one insurer to another, and may deprive the policyholder of cover in the event of non-compliance. And Sophie Di Meglio reminds us: *"It is important to read the contracts in full, which can be complex for a novice. A good solution is to seek advice from a broker, all the more so as insurers' criteria and terms evolve over time, in particular owing to the exponential increase in the number of cyber attacks over the past 2 years."*

The following are also not covered: expenses for new elements introduced as a result of an incident (e.g. software or IT system upgrades), costs and losses related to a lack of capital caused by an insured loss, and items covered by a Directors' Civil Liability policy.

Sophie Di Meglio adds: *"Some professional sectors considered to be highly exposed to cyber risk are in fact excluded by insurers. This is the case for companies that generate the majority of their sales on the Internet, IT services providers, "critical" infrastructures such as telecom companies, medical institutions or water suppliers, etc."*

## What an insurer will ask you

Generally, the company will be asked to fill out an underwriting questionnaire. Some insurance companies will not, however, require such questionnaire if it is a matter of extending an existing Objects or Civil Liability policy.

Before agreeing to insure a business, insurance companies pay particular attention to several points such as regular staff training on data protection and security, the type and amount of sensitive data processed, regular updates, malware protection, network security and multi-factor authentication, data backup and recovery, and its response plan and testing.

N.B.: just one previous incident may be sufficient for the company to be ineligible for cyber insurance!

## Cyber insurance to help prevention

Data protection should be a top priority for boards of directors and executive committees. They could be accused of lacking or having insufficient cyber risk management (with reference to Articles 717 and 754 of the Code of Obligations). Cyber insurance is an effective tool for prevention. The underwriting conditions imposed by insurance companies are ultimately the measures that every company today should already have set up to combat cyber attacks effectively.

INTERVIEW

# Cyber risk - a matter that concerns everyone in a company

**Marie de Fréminville** is an expert in governance and risk management. After a career in large international companies, she is now contributing her experience for the benefit of Swiss companies at her consulting firm Starboard Advisory. She is also the Vice President of the Swiss Circle of Women Directors.

**Is cyber risk properly taken into account by companies?**
*Most SMEs take measures to mitigate cyber risk. However, they are not immune to attack. For cybercriminals, it's easier to hack into SMEs, which lack dedicated resources, and obtain the payment of a ransom. Moreover, they are the gateway for reaching their clients with whom they are connected.*

**Cyber risk is not just an IT issue. It is also part managers' responsibility How can their awareness be raised?**
*Managers are responsible for the company's sustainability. A cyber attack can have a serious financial and reputational impact. Since security vulnerability is of human origin in 95% of cases, it is essential for everyone to receive training. IT tools are necessary, but not sufficient: managers must identify the critical assets to be protected, organise matters, set up processes, rules and a system of regular review, and prepare themselves to manage a forthcoming crisis.*

**What are the future challenges of cyber security?**
*There will be an ever-growing number of attacks. Cybersecurity is based on risk management, crisis anticipation, the implementation of resources, especially human resources, and the development of a mindset in all organisations (the risk is systemic!). As with the automobile sector, safety will improve with reliable equipment, technical verifications, a driver's license obtained on the basis of training, a highway code and supervision of the application of standard rules.*

## Managers and board members, an ever-increasing risk of liability

If you are a company manager or a member of the board... Did you know that you may incur personal civil liability in the exercise of your duties? If you are held liable, your personal assets may be used to pay compensation. There are many grounds on which your liability may be sought, and your claimants may be shareholders, the company itself, regulatory authorities, creditors, competitors, clients or your employees.

There are solutions for you to protect yourself. To find out more about them, please watch the webinar that we organised on 9 March, which brought together lawyers, experts in directors' liability, cyber security and governance.

To watch the replay of our webinar (in French only) please go to: https://www.swissriskcare.ch/les-webinaires.

Take part in our readership survey

**Are you an Insurance Inside reader?**

**Your opinion is important to us!**

Please take 5 minutes to answer these few questions which you can see by flashing the QR Code.

**Impressum**
Publisher: Swiss Risk & Care • insurance-inside@swissriskcare.ch - T +41 58 178 85 85 • Director of Publishing: David Cochet • Publishing Manager: Valérie Cruchet
Printing: Imprimerie Baudat, L'Orient • Photo credit: Swiss Risk & Care, iStock by Getty, Céline Michel, studioregard.ch.